

ANTIVIRUS

ANTISPYWARE

ANTIROOTKIT

ANTIPHISHING

ANTISPAM

PARE-FEU

CONTRÔLE PARENTAL

BitDefender Internet Security 2008

Manuel d'utilisation

BitDefender

Notice Légale

Avertissement. Ce produit et sa documentation sont protégés par copyright. Les informations de ce document sont données à titre indicatif, sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs ne pourront être tenu responsables envers quiconque de toute perte ou dommage occasionné, ou supposé occasionné, directement ou indirectement par les informations contenues dans ce document.
Ce manuel contient des liens vers des sites web de tiers qui ne sont pas sous le contrôle de BITDEFENDER, et BITDEFENDER n'est pas responsable du contenu de ces sites. Si vous accédez à un l'un des sites web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. BITDEFENDER indique ces liens uniquement à titre informatif, et l'inclusion de ce lien n'implique pas que BITDEFENDER assume ou accepte la responsabilité du contenu de ce site web d'un tiers.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques enregistrées ou non dans ce document sont la propriété unique de leur propriétaire respectif.

Table des matières

Accord de licence

Si vous n'acceptez pas les termes et conditions n'installez pas ce logiciel. En choisissant “J'accepte”, “Ok”, “Continuer”, “Oui” ou en installant ou utilisant le logiciel de quelque manière que ce soit, vous confirmez que vous comprenez parfaitement et acceptez les termes et conditions de cette licence.

Les termes de cette licence incluent les Solutions et Service BitDefender pour votre usage personnel, y compris les documentations relatives aux produits, les mises à jour et mises à niveau des applications ou les services qui vous sont proposés dans le cadre de la licence, ainsi que toute reproduction de ces éléments.

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et BITDEFENDER pour l'usage du produit de BITDEFENDER identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation "en ligne" ou électronique ("BitDefender"), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord.

Si vous n'acceptez pas les termes de cette licence, n'installez pas ou n'utilisez pas BitDefender.

Accord de licence BitDefender. BitDefender est protégé par les lois du copyright et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités concernant la propriété intellectuelle. BitDefender est licencié et non pas vendu.

DROITS DE LICENCE. Ce logiciel restant la propriété de BITDEFENDER, vous et vous seul disposez néanmoins de certains droits d'utilisation non exclusifs et non transférables, une fois l'accord de licence accepté. Vos droits et obligations relatifs à l'utilisation de ce logiciel sont les suivants :

LOGICIEL : Vous pouvez installer et utiliser BitDefender, sur autant d'ordinateurs que nécessaire dans le cadre de la limitation imposée par le nombre d'utilisateurs ayant une licence. Vous pouvez réaliser une copie à des fins de sauvegarde.

ACCORD DE LICENCE POUR ORDINATEUR. Cette licence s'applique au logiciel BitDefender qui peut être installé sur un ordinateur unique ne proposant pas de service en réseau. Chaque utilisateur
principal peut utiliser ce logiciel sur un ordinateur unique et peut réaliser une copie de sauvegarde sur un support différent. Le nombre d'utilisateurs principal correspond au nombre d'utilisateurs définit dans l'accord de licence.

DUREE DE LA LICENCE. La licence accordée ci-dessus commencera au moment où vous installez, copiez ou utilisez de toute autre manière BitDefender pour la première fois et expirera à la fin de la période pour laquelle la licence a été acquise.

EXPIRATION. Le produit cessera de fonctionner immédiatement à la date d’expiration de la licence.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par BITDEFENDER comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur. Les termes et conditions de cette licence annule et remplace tout accord préalable ayant pu exister entre vous et BITDEFENDER concernant un produit complet ou un produit mis à jour.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de BITDEFENDER. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de
découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. BITDEFENDER garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par BITDEFENDER du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. BITDEFENDER ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur. BITDEFENDER REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QU'ELLE SOIT EXPRESSE OU IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES, QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

A l'exception des termes définis dans cet accord de licence, BITDEFENDER refuse toute autre forme de garantie, explicite ou implicite en rapport avec le produit, ses améliorations, sa maintenance, ou son support ainsi que tout autre matériel relatif (tangible ou intangible) ou service fournit par celui ci.
BITDEFENDER refuse explicitement toutes garanties et conditions incluant, sans limitation, les garanties liées à la commercialisation, l’adaptation à un emploi particulier, la non interférence, la précision des données, la précision de contenus d'informations, l’intégration système, et la non violation des droits d'une tierce partie en filtrant, désactivant ou supprimant un logiciel, spyware, adware, des cookies, des emails, des documents, une publicité ou un autre produit du même type, d'un telle tierce partie, quel que soit leur mode d'utilisation.
REFUS DES DOMMAGES. Toute personne qui utilise, teste ou évalue BitDefender accepte les risques qu’il peut encourir concernant la qualité et la performance de

BitDefender. En aucun cas BITDEFENDER ne sera tenu responsable à votre égard de tout dommage particulier direct ou indirect, de réclamations liées à une perte quelconque découlant de l'utilisation ou de l'incapacité d'utiliser le logiciel même si BITDEFENDER a été avisé de l'éventualité de tels dommages. CERTAINS ETATS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DE RESPONSABILITE EN CAS DE DOMMAGE. LA REGLE EDICTEE CI-DESSUS CONCERNANT LES LIMITATIONS OU EXCLUSIONS CITEES PEUT NE PAS S'APPLIQUER A VOTRE CAS - QU'ELLES QUE SOIENT LES CONDITIONS LA REPONSABILITE DE BITDEFENDER NE POURRA EXCEDER LE MONTANT QUE VOUS AVEZ PAYE POUR BITDEFENDER. Les limitations édictées ci dessus s'appliqueront que vous acceptiez ou non d'utiliser, d'évaluer ou de tester BitDefender.

INFORMATION IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS PREVU POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. La seule juridiction compétente en cas de désacord concernant cet accord de licence sera la Cour de justice de Roumanie.

Les prix, les coûts et les frais d'usage de BitDefender peuvent changer sans que vous en soyez prévenu.

Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

BitDefender et le logo de BitDefender sont des marques déposées de BITDEFENDER. Toutes les autres marques et produits associés appartiennent à leurs propriétaires respectifs.

La licence prendra fin immédiatement sans qu'il soit besoin de vous avertir si vous ne respectez pas une ou plusieurs des conditions édictées dans cet accord. Il ne vous sera pas possible de demander un remboursement de la part de BITDEFENDER ou d'un de ses représentants en cas de cloture de cette licence. Les termes et conditions de respect de confidentialité et leurs restrictions doivent rester
de mise même après la fin du contrat.

BITDEFENDER s'autorise à revoir quand il le souhaite les termes de cette licence, ceux ci s'appliqueront automatiquement aux produits distribués qui incluent les termes modifiés. Dans l'éventualité d'une invalidité d'une partie de cet accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise édité par BITDEFENDER sera déclarée valide. En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise éditée par BITDEFENDER sera déclarée valide.

Contact BITDEFENDER : Rue Fabrica de Glucoza, No. 5, Code postal 020331 - Sector 2, Bucarest, Roumanie, ou au Tel No : +40-21-2330780 ou Fax : +40-21-2330763, adresse e-mail :
<office@bitdefender.com>.

1. Installation de BitDefender Internet Security 2008

La rubrique **Installation de BitDefender Internet Security 2008** de ce Manuel d'utilisation contient les thèmes suivants :
• Configuration système
• Etapes d'installation
• Assistant initial de démarrage
• Mise à jour majeure
• Supprimer, réparer ou modifier BitDefender

1.1. Configuration requise

Pour assurer un fonctionnement correct du produit, vérifiez avant l'installation que l'un des systèmes d'exploitation suivants fonctionne sur votre ordinateur et que vous disposez de la bonne configuration :
• **Plateforme** - Windows 2000/XP SP2 32 & 64b/Vista 32 & 64b ; Internet Explorer 6.0 (ou supérieur)
• Clients de messagerie pris en charge : Microsoft Outlook 2000 / 2003 / 2007 ; Microsoft Outlook Express ; Microsoft Windows Mail ; Thunderbird 1.5 et 2.0

Windows 2000

• Processeur 800 MHz ou supérieur
• Mémoire minimum 256Mo de RAM (512Mo recommandés)
• Au moins 60Mo d'espace disque disponible.

Windows XP

• Processeur 800 MHz ou supérieur
• Mémoire minimum : 512Mo de RAM (1 Go recommandés)
• Au moins 60Mo d'espace disque disponible.

Windows Vista

• Processeur 800 MHz ou supérieur
• Mémoire minimum : 512Mo de RAM (1 Go recommandés)
• Au moins 60Mo d'espace disque disponible.

1.2. Etapes d'installation

Introduisez le CD dans votre lecteur. Un écran d'accueil apparaîtra au bout de quelques secondes vous proposant notamment le choix de la langue.
Avant de lancer l'assistant de configuration, BitDefender recherche les nouvelles versions du programme d'installation. Si une nouvelle version est disponible, vous êtes invité à la télécharger. Cliquez sur **Oui** pour télécharger la nouvelle version ou sur **Non** pour continuer à installer la version disponible sur le CD.



Etapes d'installation
Voici les étapes à suivre pour installer BitDefender Internet Security 2008 :

1. Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l'installation.
2. Cliquez sur **Suivant**.

BitDefender vous prévient si il y a déjà un autre antivirus installé sur votre ordinateur. Cliquez sur **Supprimer** pour désinstaller le produit correspondant. Si vous souhaitez poursuivre sans supprimer le produit détecté, cliquez sur **Suivant**.

Avertissement
Il est fortement recommandé de désinstaller les autres antivirus avant d'installer BitDefender. Faire fonctionner plusieurs antivirus sur le même ordinateur le rend généralement inutilisable.

3. Merci de lire l'Accord de Licence, sélectionnez **J'accepte les termes de l'Accord de Licence** et cliquez sur **Suivant**. Si vous n'acceptez pas ces conditions, sélectionnez **Annuler**. Le processus d'installation sera abandonné et vous sortirez de l'installation.
4. Par défaut, BitDefender Internet Security 2008 est installé dans le répertoire suivant : C :\Program Files\BitDefender 2008. Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et sélectionnez le répertoire où vous souhaitez installer BitDefender Internet Security 2008.

Cliquez sur **Suivant**.

5. Sélectionnez les options du processus d'installation. Certaines sont sélectionnées par défaut.

• **Ouvrir le fichier lisezmoi** - pour ouvrir le fichier lisez moi à la fin de l'installation.

- **Créer un raccourci sur le bureau** - pour mettre un raccourci BitDefender internet security 2008 sur le bureau à la fin de l'installation.
- **Éjecter le CD après l'installation** - pour que le CD soit éjecté à la fin de l'installation, cette option apparaît au moment de l'installation du produit.
- **Désactiver le pare-feu Windows** - pour désactiver le pare-feu Windows.



Important
Nous vous recommandons de désactiver le pare-feu Windows, car BitDefender internet security 2008 comprend déjà un pare-feu avancé. L'exécution simultanée de deux pare-feu sur le même ordinateur peut provoquer des problèmes.

- Désactiver Windows Defender - pour désactiver Windows Defender ; cette option n'est disponible que sous Windows Vista.

Cliquez sur **Installer** afin de commencer l'installation du produit.



Important
Pendant la procédure d'installation un assistant apparaîtra. Il vous aidera à enregistrer votre BitDefender internet security 2008, à créer un compte et à paramétrer BitDefender pour lancer d'importantes tâches de sécurité.
Complétez l'assistant d'installation pour passer à l'étape suivante.

6. Cliquez sur **Terminer** pour compléter l'installation du produit. Si vous avez accepté les paramètres par défaut pour le répertoire d'installation, un nouveau répertoire du nom de BitDefender est créé dans Program Files contenant le sous-répertoire BitDefender 2008.

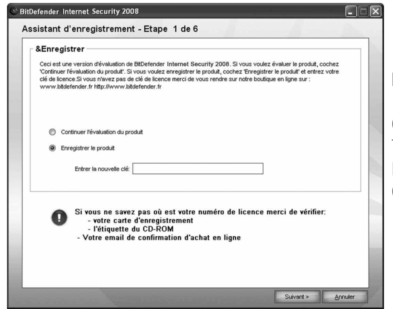


Note
Il vous sera peut être demandé de redémarrer votre système pour terminer le processus d'installation.

1.3. Assistant de première installation

Un assistant apparaîtra pendant la procédure d'installation. L'assistant vous aide à enregistrer votre BitDefender internet security 2008, à créer un compte et à paramétrer BitDefender pour lancer d'importantes tâches de sécurité. Compléter cet assistant n'est pas obligatoire. Cependant, nous vous recommandons de le faire pour gagner du temps et vous assurer que votre système est sain même avant l'installation de BitDefender internet security 2008.

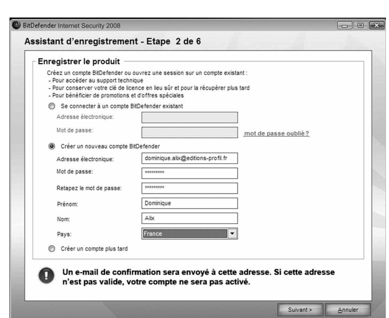
1.3.1. Etape 1 sur 6 - Enregistrer BitDefender internet security 2008



Enregistrement du Produit

Choisissez **Enregistrer le produit** pour enregistrer **BitDefender internet security 2008.**
Tapez la clé de licence dans le champ **Entrer la nouvelle clé.**
Pour continuer à évaluer le produit, sélectionnez Continuer l'évaluation du produit.
Cliquez sur **Suivant.**

1.3.2. Etape 2 sur 6 - Création d'un compte BitDefender



Création de compte

Je n'ai pas de compte BitDefender

Pour bénéficier du support technique gratuit et d'autres services, il faut créer un compte BitDefender. Sélectionnez **Créer mon compte BitDefender** et entrez les informations demandées. Les informations
communiquées ici resteront confidentielles.



Note
Si vous voulez créer un compte plus tard, choisissez l'option correspondante.

Entrez une adresse email valide dans le champ E-mail. Entrez votre mot de passe dans le champ Mot de passe. Confirmez le mot de passe dans le champ Retapez Mot de passe. Utilisez l'adresse mail et le mot de passe pour vous connecter à votre compte sur http ://myaccount.bitdefender.com



Note
Votre mot de passe doit comporter au moins quatre caractères.

Entrez vos noms et prénoms et choisissez votre pays.
Pour créer votre compte vous devez d'abord activer votre adresse e-mail. Vérifiez votre messagerie et suivez les instructions reçues dans l'email qui vous a été envoyé par le service d'enregistrement BitDefender. Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

J'ai déjà un compte BitDefender
Si vous avez déjà un compte BitDefender, entrez votre adresse email et le mot de passe de votre compte. Si vous tapez un mot de passe incorrect, il vous sera demandé de le ressaisir quand vous cliquerez sur **Suivant**. Cliquez sur **Ok** pour ressaisir votre mot de passe ou sur **Annuler** pour sortir de l'assistant.
Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

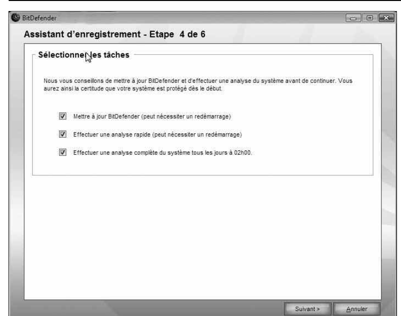
Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

1.3.3. Etape 3 sur 6 - En savoir plus sur le RTVR



Informations sur le RTVR
Cliquez sur Suivant pour continuer ou sur Annuler pour quitter l'assistant.

1.3.4. Etape 4 sur 6 - Sélectionner les tâches à lancer



Sélection des tâches
Paramétrez BitDefender internet security 2008 pour lancer les tâches de sécurité importantes pour votre ordinateur. Les options suivantes sont disponibles :

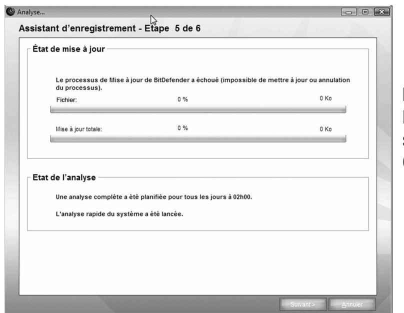
- **Mettre à jour les moteurs BitDefender (peut nécessiter un redémarrage)** - une mise à jour des moteurs de BitDefender aura lieu pendant la prochaine étape pour protéger votre ordinateur contre les dernières menaces.
- **Lancer une analyse rapide (peut nécessiter un redémarrage)** - Une analyse rapide sera lancée pendant la prochaine étape afin que BitDefender s'assure que les fichiers contenus dans le dossier Windows and Program Files ne sont pas infectés.
- **Lancer une analyse complète de l'ordinateur tous les jours à 02h00** - Lance une analyse complète du système tous les jours à 02h00.



Important
Il est fortement recommandé d'activer ces options avant de passer à l'étape suivante pour assurer la sécurité de votre système.

Si vous sélectionnez uniquement la dernière option ou aucune option, vous passerez l'étape suivante.
Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

1.3.5. Etape 5 sur 6 - Merci d'attendre la fin de la tâche



Etat d'avancement de la tâche
Merci d'attendre la fin de la tâche. Vous pouvez vérifier ici l'avancement de la tâche que vous avez sélectionnée lors de l'étape précédente.
Cliquez sur **Suivant** pour continuer ou sur **Annuler** pour quitter l'assistant.

1.3.6. Etape 6 sur 6 - Voir le récapitulatif



Terminer
Il s'agit de l'étape finale de l'assistant de configuration.
Cliquez sur **Terminer** pour terminer l'assistant et continuer avec l'installation du produit.

1.4. Mise à jour majeure

La procédure de mise à jour majeure peut se faire ainsi : **• Installer sans désinstaller les versions précédentes - pour BitDefender v8 ou plus récent, sauf Internet Security.** Double-cliquez sur le fichier d'installation et suivez l'assistant décrit dans la section "Etapes d'installation" (p. 1).

Important
Durant le processus d'installation, un message d'erreur causé par le Filespy service, apparaîtra.

Cliquez sur **OK** pour continuer l'installation.

• Désinstallez votre ancienne version et installez la nouvelle - pour toutes les versions BitDefender. En premier lieu, vous devez désinstaller la version précédente, redémarrer l'ordinateur et installer la nouvelle comme décrit dans la rubrique **"Etapes d'installation" (p. 1).**



Important
En cas de mise à niveau de BitDefender v8 ou supérieur, nous vous recommandons d'enregistrer les paramètres BitDefender, la Liste des amis et la Liste des spammeurs. Une fois le processus de mise à niveau terminé, vous pourrez les charger.

1.5. Supprimer, réparer ou modifier BitDefender

Si vous souhaitez réparer ou supprimer **BitDefender internet security 2008,** suivez le chemin depuis le menu Démarrer de Windows : **Démarrer _ Programmes _ BitDefender 2008 _ Réparer ou supprimer.**

Il vous sera demandé une confirmation de votre choix en cliquant sur Suivant. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir :
• Réparer - pour réinstaller tous les composants choisis lors de l'installation précédente.



Important
Avant la réparation du produit, nous vous recommandons d'enregistrer la Liste des amis et la Liste des spammeurs. Vous pouvez également enregistrer les paramètres BitDefender et la base de données bayésienne. Une fois le processus de réparation terminé, vous pourrez les télécharger à nouveau.

Si vous décidez de réparer BitDefender, une nouvelle fenêtre s'affiche. Cliquez sur **Réparer** pour lancer le processus.
Redémarrez l'ordinateur comme demandé puis cliquez sur "Redémarrer l'ordinateur" lorsque demandé et, après cela, cliquez sur Installer pour réinstaller BitDefender internet security 2008. Une fois l'installation achevée, une nouvelle fenêtre s'affiche. Cliquez sur **Terminer**.
• **Supprimer** - pour supprimer tous les composants installés.



Note
Nous vous recommandons de sélectionner **Supprimer** *pour que la réinstallation soit saine.*

Si vous décidez de supprimer BitDefender, une nouvelle fenêtre s'affiche.



Important
Si vous supprimez BitDefender, votre ordinateur ne sera plus protégé contre les virus, les spywares et les pirates. Si vous souhaiter activer Windows Firewall et Windows Defender (uniquement sur Windows Vista) après la désinstallation de BitDefender, cochez les cases correspondantes.

Cliquez sur **Supprimer** pour désinstaller BitDefender internet security 2008 de votre ordinateur. Pendant ce processus, votre avis vous sera demandé. Veuillez cliquer sur **OK** pour répondre à une enquête en ligne qui comprend seulement cinq questions. Si vous ne souhaitez pas répondre à cette enquête, cliquez simplement sur **Annuler**.
Une fois la désinstallation achevée, une nouvelle fenêtre s'affiche. Cliquez sur **Terminer**.



Note
A l'issue de la désinstallation, nous vous recommandons de supprimer le sous-répertoire BitDefender du répertoire Program Files.

Une erreur est survenue lors de la désinstallation de BitDefender
Si une erreur survient lors de la désinstallation de BitDefender, le processus est abandonné et une nouvelle fenêtre s'affiche. Cliquez sur **Exécuter l'outil de désinstallation** pour vérifier que BitDefender a bien été complètement supprimé. L'outil de désinstallation efface tous les fichiers ainsi que les clés d'enregistrement qui n'ont pas été supprimés lors de la désinstallation automatique.

2. Pour commencer

Une fois BitDefender installé, votre ordinateur est protégé. Vous pouvez ouvrir le Centre de sécurité BitDefender à tout moment pour vérifier le statut de sécurité de votre système, prendre des mesures préventives ou configurer entièrement le produit.

Pour accéder au Centre de sécurité BitDefender, utilisez le menu Démarrer de Windows en suivant le chemin **Démarrer ➠ Programmes ➠ BitDefender 2008 ➠ BitDefender internet security 2008** ou, plus rapide, en double cliquant sur l' icône BitDefender dans la barre d'état système.



Centre de sécurité BitDefender

Le Centre de sécurité BitDefender comporte deux zones :

• La zone **Statut** : contient des informations sur les problèmes de vulnérabilité de votre ordinateur en matière de sécurité et vous aide à les résoudre. Vous pouvez facilement voir combien de problèmes affectent votre ordinateur. En cliquant sur le bouton rouge correspondant **Tout réparer**, les problèmes de vulnérabilité de votre ordinateur seront directement résolus ou le système vous guidera pour vous aider à les résoudre facilement. Par ailleurs, quatre boutons de statut correspondant aux quatre niveaux de sécurité sont disponibles. Les boutons de statut verts indiquent qu'il n'y a pas de risque. Les boutons jaunes ou rouges indiquent des risques moyens ou élevés. Cliquez sur le bouton jaune/rouge, puis sur le bouton **Réparer** pour les supprimer un par un ou sur le bouton **Tout réparer maintenant**. Le bouton gris indique un composant non configuré.

• **Zone des tâches rapides :** vous aide à prendre les mesures préventives indispensables à la protection de votre système et de vos données. Cette zone comprend trois onglets correspondant à trois types d'actions de sécurité. Elle vous permet de mettre à jour votre produit, d'analyser votre ordinateur, d'enregistrer ou de restaurer vos données, de défragmenter votre disque, de nettoyer les fichiers Internet temporaires et les cookies, de nettoyer et de restaurer les registres, de rechercher les doublons et de supprimer des fichiers en toute sécurité.

Le Centre de sécurité BitDefender comporte en outre de nombreux raccourcis utiles.

Lien	Description
Mon compte	Ouvre la page de votre compte BitDefender.
Enregistrer	Ouvre l'assistant d'enregistrement.
Aide	Ouvre le fichier d'aide.
Support	Ouvre la page Web du support BitDefender.
Paramètres	Ouvre la console des paramètres avancés.
Historique	Ouvre une fenêtre présentant l'historique et les événements BitDefender.

Pour gérer l'intégralité du produit plus rapidement, vous pouvez aussi utiliser l'icône BitDefender située dans la barre d'état système.



Menu contextuel

Double-cliquez sur cette icône pour ouvrir le Centre de sécurité BitDefender. Si vous effectuez un clic droit sur cette icône, le menu contextuel qui apparaît vous permettra de gérer le produit BitDefender plus rapidement.

- **Afficher** - ouvre le Centre de sécurité BitDefender.
- **Aide** - ouvre la documentation d'aide électronique.
- **À propos** - ouvre la page Web BitDefender.
- **Tout réparer** - vous aide à résoudre les problèmes de vulnérabilité de votre ordinateur en matière de sécurité.
- **Activer le mode Jeu** - désactive les alertes et les notes sur l'écran et règle votre niveau de protection en temps réel sur Tolérant.
- **Ouvrir les paramètres avancés** - permet d'accéder à la console des paramètres avancés.

2.1. Analyse Manuelle BitDefender

Si vous souhaitez analyser rapidement un répertoire donné, vous pouvez utiliser l'analyse manuelle BitDefender

Pour accéder à l'Analyse Manuelle BitDefender, suivez le chemin suivant depuis le menu Démarrer de Windows : **Démarrer ➠ Programmes ➠ BitDefender 2008 ➠ Analyse Manuelle BitDefender**.

Il vous suffit de sélectionner le répertoire souhaité et de cliquer sur **OK**.

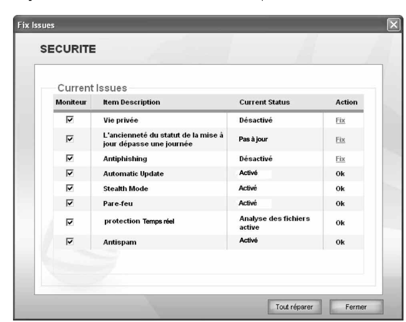
3. Statut de sécurité

Le statut de sécurité affiche une liste organisée de façon systématique et facilement gérable regroupant les problèmes de vulnérabilité de votre ordinateur en matière de sécurité. BitDefender Internet Security 2008 vous avertit de tout problème pouvant affecter la sécurité de votre ordinateur.

Il existe quatre boutons liés au statut de sécurité :
- **SÉCURITÉ RÉSEAU**
- **SÉCURITÉ**
- **CONFIDENTIALITÉ**
- **CONTROLE PARENTAL**

Par ailleurs, vous pouvez voir sur la gauche le nombre de problèmes affectant la sécurité de votre système et un bouton rouge **Tout réparer.** Les quatre boutons de statut peuvent s'afficher en vert, jaune, rouge ou gris en fonction du niveau de protection en cours.
- **Vert** indique un risque faible pour votre ordinateur.
- **Jaune** indique un risque moyen pour votre ordinateur.
- **Rouge** indique un risque élevé pour votre ordinateur.
- **Gris** indique un composant non configuré.

Les problèmes de sécurité peuvent être facilement résolus par un simple clic sur le bouton **Tout réparer.** Vous verrez s'afficher la liste des problèmes de sécurité et une courte description de leur statut. Pour ne résoudre qu'un problème de sécurité spécifique, cliquez sur le bouton **Réparer** correspondant. Le problème sera soit directement résolu, soit résolu après avoir suivi les étapes d'un assistant. Si vous choisissez de résoudre tous les problèmes de sécurité, cliquez sur **Tout réparer maintenant** et suivez les étapes de l'assistant correspondant.



Problèmes de sécurité
Pour résoudre ces problèmes de sécurité ultérieurement, cliquez sur **Fermer**.

Important
Pour chaque problème, une case est cochée par défaut. Si vous ne souhaitez pas qu'un problème spécifique soit pris en compte lors de l'évaluation du niveau de risque, décochez la case correspondante. Veuillez utiliser cette option avec circonspection, il est très simple d'augmenter le niveau de risque auquel votre ordinateur est exposé.

3.1. Bouton de statut de la sécurité réseau

Si le bouton de statut est vert, vous n'avez aucune inquiétude à avoir. Par contre, si le bouton est rouge, votre ordinateur est exposé à un niveau de risque élevé. Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	Couleur
Le pare-feu est désactivé.	**Rouge**
Le mode furtif est désactivé.	**Rouge**
La connexion sans fil n'est pas sécurisée.	**Rouge**

Pour résoudre les problèmes de sécurité, suivez ces étapes:

1. Cliquez sur le bouton de statut de la sécurité réseau.
2. Cliquez soit sur les boutons Réparer pour les résoudre un à un, soit sur le bouton Tout réparer maintenant pour toutes les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

3.2. Bouton du statut de sécurité

Si le bouton du statut de sécurité est vert, vous n'avez aucune inquiétude à avoir. S'il est jaune, rouge ou gris, cela signifie que votre ordinateur est exposé à un risque moyen ou élevé. La couleur des boutons de statut peut se modifier non seulement lorsque vous configurez les paramètres pouvant affecter la sécurité de votre ordinateur, mais aussi si vous oubliez d'effectuer des tâches importantes. Si votre système n'a pas été analysé depuis longtemps, par exemple, le bouton du statut de sécurité est affiché en jaune. S'il ne l'a pas été depuis très longtemps, le bouton est affiché en rouge.

Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	Couleur
Votre système n'a pas été analysé depuis longtemps.	**Jaune**
Votre système n'a pas été analysé depuis très longtemps.	**Rouge**
La protection en temps réel est désactivée.	**Rouge**
Le niveau de protection antivirus est réglé sur Tolérant.	**Jaune**
La mise à jour automatique est désactivée.	**Rouge**
La dernière mise à jour remonte à plus de un jour.	**Rouge**
L'antispam est désactivé.	**Gris**

Pour résoudre les problèmes de sécurité, suivez ces étapes :

1. Cliquez sur le bouton du statut de sécurité.
2. Cliquez soit sur les boutons **Réparer** pour les résoudre un à un, soit sur le bouton **Tout réparer maintenant** pour tous les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

3.3. Bouton de statut de la confidentialité

Si le bouton du statut est vert, vous n'avez aucune inquiétude à avoir. Par contre, si le bouton est rouge ou gris, votre ordinateur est exposé à un niveau de risque élevé.

Le tableau ci-dessous vous indique quels sont les éléments pris en compte dans l'évaluation des risques de sécurité.

Problème de sécurité	Couleur
La protection de la confidentialité est configurée et activée	**Vert**
La protection de la confidentialité est configurée et désactivée	**Rouge**
La protection de la confidentialité n'est pas configurée	**Gris**

Pour résoudre les problèmes de sécurité, suivez ces étapes:

1. Cliquez sur le bouton de statut de la confidentialité.
2. Cliquez soit sur les boutons **Réparer** pour les résoudre un à un, soit sur le bouton **Tout réparer maintenant** pour toutes les résoudre en un seul clic.
3. Si un problème de sécurité n'a pas pu être directement résolu, suivez l'assistant.

3.4. Bouton du statut du Contrôle parental

Si le bouton du statut de sécurité est vert, le Contrôle parental est activé. S'il est gris, cela signifie qu'il est désactivé.
Pour activer le Contrôle parental, cliquez sur le bouton de statut correspondant, puis cliquez sur le bouton **Configurer**.

4. Tâches rapides

Sous les quatre boutons de statut se trouve la zone de tâches prédéfinies :

4.1 Sécurité

BitDefender comporte un module Sécurité qui vous permet de maintenir votre système à jour et protégé contre les virus.
Pour accéder au module Sécurité, cliquez sur l'onglet Sécurité.
Voici les différents boutons proposés :
- **Mettre à jour** - lance une mise à jour silencieuse.
- **Analyser mes documents** - lance une analyse rapide de vos documents et paramètres.
- **Analyse complète du système** -lance une analyse complète de votre ordinateur.

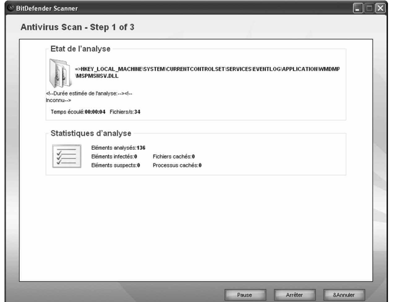
4.1.1. Mise à jour

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

4.1.2. Moteur d'analyse BitDefender

Lorsque vous lancez un processus d'analyse sur demande, que ce soit une analyse rapide ou complète, le moteur d'analyse BitDefender apparaît.
Suivez cette procédure en trois étapes pour effectuer le processus d'analyse :

Étape 1 sur 3 - Analyse
BitDefender commence à analyser les objets sélectionnés.



Analyse en cours
Le statut et les statistiques de l'analyse s'affichent (vitesse d'analyse, temps écoulé, nombre d'objets analysés / infectés / suspects / cachés, etc.).



Note
L'analyse peut durer un certain temps, suivant la complexité de l'analyse. Pour suspendre temporairement le processus d'analyse, cliquez sur Pause. Pour reprendre l'analyse, cliquez sur Reprendre.

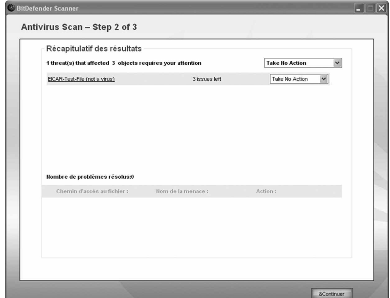
Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter** et **Oui**. Vous vous retrouverez alors à la dernière étape de l'assistant.



Note
Lorsque des fichiers suspects seront détectés durant l'analyse, vous serez invité à les envoyer au laboratoire BitDefender.

Patientez jusqu'à ce que BitDefender ait terminé l'analyse.

Étape 2 sur 3 - Sélectionner des actions
Une fois l'analyse terminée, une nouvelle fenêtre apparaît affichant les résultats de l'analyse.



Actions
Le nombre de problèmes de sécurité affectant votre système est indiqué.
Les problèmes de sécurité sont affichés en groupes. Cliquez sur "**+**" pour ouvrir un groupe ou sur "**-**" pour fermer un groupe.
Vous pouvez sélectionner une action globale à mener pour chaque groupe de problèmes de sécurité ou sélectionner des actions spécifiques pour chaque problème.
Les options suivantes peuvent s'afficher dans le menu :
Action Description
Ne pas mener d'action Aucune action ne sera menée sur les fichiers détectés.
Désinfecter Pour désinfecter un fichier infecté.
Supprimer Supprime les fichiers détectés.
Démasquer Rend les objets cachés visibles.
Cliquez sur **Réparer** pour appliquer les actions spécifiées.

Étape 3 sur 3 - Voir les résultats

Une fois les problèmes de sécurité résolus par BitDefender, les résultats de l'analyse apparaissent dans une nouvelle fenêtre.



Récapitulatif

Le récapitulatif des résultats s'affiche.

Le fichier rapport est sauvegardé automatiquement dans la rubrique Journaux de la fenêtre Propriétés de la tâche en question.

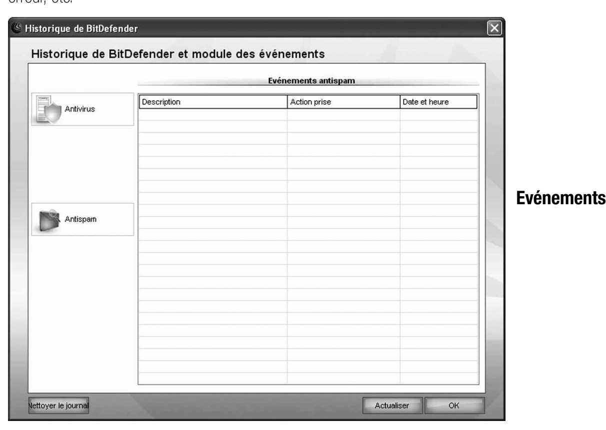


Avertissement

Dans le cas d'un problème de sécurité non résolu, nous vous recommandons de contacter le support BitDefender sur le site www.bitdefender.com.

5. Historique

Le lien **Historique** situé dans la partie inférieure de la fenêtre du Centre de sécurité BitDefender permet d'ouvrir une autre fenêtre comportant l'historique et les événements BitDefender. Cette fenêtre vous offre une vue d'ensemble des événements relatifs à la sécurité. Elle vous permet, par exemple, de vérifier facilement qu'une mise à jour a bien été effectuée, de savoir si des codes malveillants ont été détectés sur votre ordinateur, si vos tâches de sauvegarde sont exécutées sans erreur, etc.



Evénements

Les catégories suivantes, présentées à gauche, permettent de filtrer l'historique et les événements BitDefender :

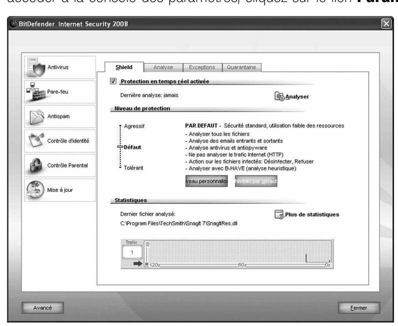
- **Antivirus**
- **Confidentialité**
- **Pare-feu**
- **Antispam**
- **Contrôle parental**
- **Mise à jour**

Une liste d'événements est proposée pour chaque catégorie. Chaque événement comporte les informations suivantes : une courte description de l'événement, l'action menée par BitDefender, la date et l'heure de l'événement. Pour obtenir plus d'informations sur un événement de la liste en particulier, double-cliquez sur cet événement.

Cliquez sur **Nettoyer le journal** pour supprimer les journaux anciens ou sur **Actualiser** pour vous assurer que les derniers journaux sont bien affichés.

6. Pour commencer

BitDefender internet security 2008 comporte une console de paramètres centralisée qui permet la configuration et la gestion avancée de BitDefender. Pour accéder à la console des paramètres, cliquez sur le lien **Paramètres** situé dans la partie inférieure du Centre de sécurité.



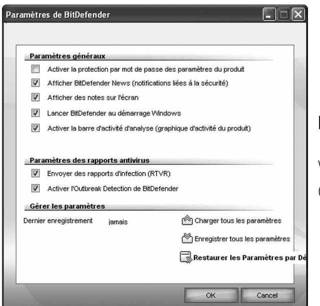
Console des paramètres

La console des paramètres est organisée par modules : **Antivirus, Firewall, Antispam, Contrôle d'identité, Contrôle parental et Mise à jour.** Cela permet de gérer facilement BitDefender selon le type de problème de sécurité à traiter.
Sur la partie gauche de la console, vous pouvez sélectionner les modules suivants :

- Antivirus - pour accéder à la fenêtre de configuration de l'**Antivirus**.
- Pare-feu - pour accéder à la fenêtre de configuration du **Pare-feu**.
- Antispam - pour accéder à la fenêtre de configuration de **l'Antispam**.
- Contrôle de l'identité - dans cette section, vous pouvez configurer le module de **Contrôle d'identité**.
- Contrôle Parental - pour accéder à la fenêtre de configuration du **Contrôle Parental**.
- Mise à jour - pour accéder à la fenêtre de configuration des **Mises à jour**.

6.1. Configuration des paramètres généraux

Pour configurer les paramètres généraux de BitDefender internet security 2008 et pour les gérer, cliquez sur **Avancé**. Une nouvelle fenêtre s'affiche.



Paramètres Généraux

Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se réduit automatiquement.

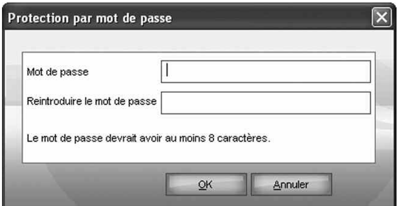
6.1.1. Paramètres Généraux

- **Activer la protection par mot de passe pour les paramètres du produit** - permet de choisir un mot de passe afin de protéger la configuration de la console de gestion BitDefender.



Note
Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres BitDefender par un mot de passe.

La fenêtre suivante apparaîtra :



Mot de passe
Entrez le mot de passe dans le champ Mot de passe, re-saisissez le dans le champ Reintroduire le mot de passe et cliquez sur OK. A présent, si vous souhaitez changer les options de configuration de BitDefender, le mot de passe vous sera demandé.



Important
Si vous avez oublié votre mot de passe vous devrez réinstaller partiellement le produit pour modifier la configuration de BitDefender.

- **Recevoir alertes de sécurité -** affiche régulièrement des informations de sécurité sur des risques de virus et/ou de failles, envoyées par les serveurs de BitDefender.

- **Afficher des notes sur l'écran** - affiche des fenêtres de notifications sur l'état de votre produit.

- **Lancer BitDefender au démarrage Windows** - lance automatiquement BitDefender au démarrage du système. Nous vous recommandons de garder cette option active.

- **Activer la barre d'analyse de l'activité (sur le graphique de l'activité du produit)** - active/désactive la barre d'analyse de l'activité.

6.1.2. Paramètres du rapport des virus

- **Envoyer des rapports de virus** - envoie aux BitDefender Labs des rapports concernant les virus identifiés sur vote ordinateur. Les informations envoyées nous servent à garder une trace des apparitions de virus. Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront uniquement le nom des virus et seront utilisées dans le seul but de créer des rapports statistiques.
- **Activer l'Outbreak Detection de BitDefender** - envoie des rapports aux BitDefender Labs à propos d'apparitions éventuelles de virus. Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront uniquement les virus potentiels et seront utilisées dans le seul but de créer des rapports statistiques.

6.1.3. Gérer les paramètres

Utilisez les boutons **Enregistrer tous les paramètres** / **Charger tous les paramètres pour sauvegarder** / **Charger les paramètres établis** pour BitDefender dans un endroit spécifié. Ainsi, vous pouvez utiliser les mêmes paramètres après la réinstallation ou la réparation de votre BitDefender.



Important
Seuls les utilisateurs ayant des droits administrateurs peuvent sauvegarder et charger les paramètres.

Pour charger les paramètres par défaut, cliquez sur **Restaurer les paramètres par défaut.**

6.2. Utilisation de la barre d'activité d'analyse

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système.



Barre d'activité

Les barres vertes (la **Zone de fichiers**) montrent le nombre de fichiers analysés par seconde, sur une échelle de 0 à 50.
La barre rouge affichée dans la **Zone Internet** montre le nombre de Kbs transférés (envoyés et reçus depuis Internet) chaque seconde, sur une échelle de 0 à 100.



Note
La barre d'analyse d'activité vous informe si la protection en temps réel ou le firewall est désactivé en affichant une croix rouge sur la zone correspondante (Zone de fichiers ou Zone Internet).

Vous pouvez utiliser la Barre d'activité d'analyse pour analyser des objets. Il vous suffit pour cela de faire glisser les objets que vous souhaitez analyser et de les déposer dans cette fenêtre.



Note
Pour plus d'informations, reportez-vous à “Analyse par glisser&déposer” (p. 61).

Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**.



Note
Pour masquer complètement la fenêtre, cliquez sur Avancé dans la console des paramètres puis décochez la case Activer la barre d'activité d'analyse (graphique d'activité du produit).

7. Antivirus

BitDefender protège votre ordinateur contre tous les types de malware (virus, chevaux de Troie, spywares, rootkits, etc.). Au-delà de l'analyse classique basée sur les signatures de codes malveillants, BitDefender effectue aussi une analyse heuristique des fichiers analysés. L'analyse heuristique a pour objectif d'identifier de nouveaux virus sur la base de certains modèles et algorithmes avant qu'une définition virus ne soit détectée. De faux messages d'alerte peuvent potentiellement s'afficher. Lorsqu'un fichier de ce type est détecté, il est considéré comme étant suspect. Dans ce cas, nous vous recommandons de l'envoyer au laboratoire BitDefender pour analyse.

La protection offerte par BitDefender est divisée en deux catégories :

- **Analyse à l'accès** - empêche les nouveaux virus d'infecter votre ordinateur. Il s'agit d'un bouclier antivirus – les fichiers sont analysés au moment où l'utilisateur y accède. BitDefender analyse chaque fichier auquel un utilisateur accède ou copié sur le disque dur. BitDefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.
- **Analyse à la demande** - permet de détecter et de supprimer les malwares déjà présents dans votre système. C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que BitDefender doit analyser et BitDefender le fait – A la demande. Les tâches d'analyse permettent de créer des programmes d'analyse personnalisés qui peuvent être planifiés pour être exécutés régulièrement.

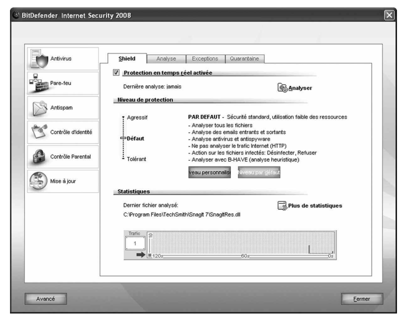
La rubrique **Antivirus** de ce Manuel d'utilisation contient les thèmes suivants :

- Analyse à l'accès
- Analyse à la demande
- Objets exclus de l'analyse
- Quarantaine

7.1. Analyse à l'accès

L'analyse à l'accès, également appelée protection en temps réel, protège votre ordinateur contre toutes les menaces de codes malveillants en analysant tous les fichiers à l'accès, les e-mails et les communications via les applications de messagerie instantanée (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Pour configurer et contrôler la protection en temps réel, cliquez sur **Antivirus > Résident** dans la console des paramètres. La fenêtre suivante apparaît :



Protection en temps réel.



Important
Pour prévenir l'infection de votre ordinateur par des virus, laissez **la protection en temps réel** activée.

Dans la partie inférieure de cette rubrique, vous pouvez voir les statistiques de **protection en temps réel** sur les fichiers et emails analysés. Cliquez sur **Plus de statistiques** si vous voulez ouvrir une fenêtre plus détaillée.

Pour lancer une analyse rapide du système, cliquez sur **Analyser**.

7.1.1. Configuration du niveau de protection

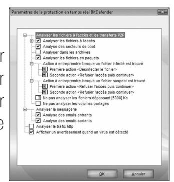
Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection :

Niveau de Protection	Description
Tolérant	Couvre les besoins de sécurité de base. La consommation de ressources système est très faible. Les programmes et emails entrants ne sont analysés que pour rechercher les virus. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes : nettoyer le fichier / refuser l'accès.
Défaut	Offre un niveau de sécurité standard. La consommation de ressources système est faible. Tous les fichiers et les emails entrants ou sortants sont analysés pour rechercher les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises contre les fichiers infectés sont les suivantes : nettoyer le fichier / refuser l'accès.
Agressif	Offre un niveau de sécurité élevé. La consommation de ressources système est modérée. Tous les fichiers, les emails entrants ou sortants et le trafic Web, sont analysés pour rechercher les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise aussi un moteur d'analyse heuristique. Les actions prises envers les fichiers infectés sont les suivantes : nettoyer le fichier / refuser l'accès.

Pour appliquer les paramètres de protection en temps réel, cliquez sur **Niveau par défaut.**

7.1.2. Personnaliser le niveau de protection



Configuration du résident

Les utilisateurs avancés peuvent utiliser les paramètres d'analyse proposés par BitDefender. Le moteur d'analyse peut être configuré pour analyser uniquement des extensions de fichiers spécifiques, pour rechercher des menaces de codes malveillants spécifiques ou pour passer les archives. Cela peut permettre de réduire considérablement la durée d'une analyse et d'améliorer la réactivité de votre ordinateur lors de l'analyse. Vous pouvez personnaliser **la protection en temps réel** en cliquant sur **Niveau personnalisé**. La fenêtre suivante apparaîtra : Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows.



Note

Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option. Vous pourrez observer que certaines options d'analyse ne peuvent pas s'ouvrir, même si un signe "+" apparaît à leur côté. La raison est que ces options n'ont pas encore été sélectionnées. Si vous les cochez, elles pourront être ouvertes.

- Sélectionnez Analyser à l'accès les fichiers et les transferts P2P pour analyser les fichiers à l'accès ainsi que les communications et échanges Peer To Peer (messageries instantanées comme ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger – logiciels de téléchargement comme Kazaa, Emule, Shareaza). Après cela, sélectionnez le type de fichiers que vous voulez analyser.

Option		Description
Analyser les fichiers	**Analyse de tous les fichiers**	Tous les fichiers seront analysés à l'accès, quel que soit leur type.
	Analyse des extensiens à risques seulement	Seuls les fichiers avec les extensions suivantes seront analysés : .exe ; .bat ; .com ; .dll ; .ocx ; .scr ; .bin ; Analyse des extensions à risques seulement :.dat ; .386 ; .vxd ; .sys ; .wdm ; .cla ; .class ; .ovl ;.ole ; .exe ; .hlp ; .doc ; .dot ; .xls ; .ppt ; .wbk ; .wiz ;.pot ; .ppa ; .xla ; .xlt ; .vbs ; .vbe ; .mdb ; .rtf ; .htm ;.hta ; .html ; .xml ; .xtp ; .php ; .asp ; .js ; .shs ; .chm ;.lnk ; .pif ; .prc ; .url ; .smm ; .pdf ; .msi ; .ini ; .csc ;.cmd ; .bas ; .eml et .nws.
	Analyse des extensions définies par l'utilisateur :	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par " ;".
	Rechercher des riskware :	Analyses contre les risques non-viraux Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée. Sélectionnez Exclure les dialers et les applications de l'analyse si vous souhaitez exclure ce genre de fichiers de l'analyse.
Analyse des secteurs de boot		Analyser les secteurs de boot du système.
Analyser dans les archives		Les archives seront également analysées. Avec cette option activée, l'ordinateur sera ralentit.
Analyser dans les fichiers compressés		Tous les fichiers compressés seront analysés
Première action		Sélectionnez à partir du menu déroulant la première action à entreprendre sur les fichiers suspicieux et infectés.
	Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit
	Désinfecter le fichier	Pour désinfecter un fichier infecté.
	Supprimer le fichier	Supprime immédiatement les fichiers infectés, sans avertissement.
	Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine.
Deuxième action		Sélectionnez à partir du menu déroulant la deuxième action à entreprendre sur les fichiers infectés, au cas où la première action échoue.
	Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
	Supprimer le fichier	Supprime immédiatement les fichiers infectés, sans avertissement.
	Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine.
Ne pas analyser les fichiers d'une taille supérieure à [x] Ko		Tapez la taille maximum des fichiers à analyser. Si vous mettez la taille à 0, tous les fichiers seront analysés.
Ne pas analyser les volumes partagés		Si cette option est activée, BitDefender n'analysera pas les volumes partagés, permettant un accès plus rapide au réseau.
		Nous vous recommandons d'activer cette option uniquement si le réseau dont fait partie votre ordinateur est protégé par un antivirus.

- Analyser le trafic de messagerie - analyse le trafic de la messagerie.

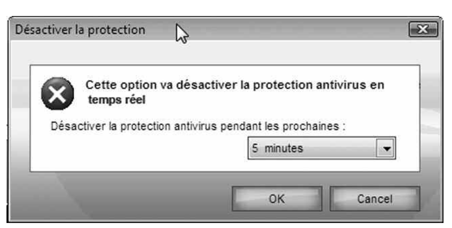
Les options suivantes sont disponibles :

Option	Description
Analyser les emails entrants	Analyser tous les emails entrants.
Analyser les emails sortants	Analyser tous les emails sortants.

• **Analyser le trafic http** - analyse le trafic http.
• **Afficher une alerte si un virus est trouvé** - une fenêtre d'alerte sera affichée lorsqu'un virus sera détecté dans un fichier ou message e-mail. Pour un fichier infecté, la fenêtre d'alerte contiendra le nom du virus, le chemin, l'action effectuée par BitDefender et un lien vers le site BitDefender où l'on peut trouver plus d'informations sur ce virus. Pour un message e-mail infecté, la fenêtre d'alerte contiendra également des informations sur l'expéditeur et le destinataire. Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera à envoyer ce fichier aux BitDefender Labs pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.
Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

7.1.3. Désactivation de la protection en temps réel

Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît.

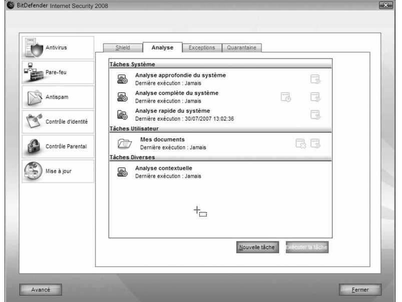


Désactiver la protection en temps réel
Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la protection en temps réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

Avertissement
Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la protection en temps réel pendant le moins de temps possible. Si la protection en temps réel est désactivée, vous ne serez pas protégé contre les menaces de codes malveillants.

7.2. Analyse à la demande

L'objectif principal de BitDefender est de conserver votre ordinateur sans virus. Cela se fait avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système. Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de BitDefender. Et il encore plus prudent d'analyser régulièrement votre ordinateur contre les virus. Pour configurer et lancer une analyse sur demande, cliquez sur **Antivirus > Analyse** dans la console des paramètres. La fenêtre suivante apparaît :



Tâches d'analyse
L'analyse sur demande est basée sur les tâches d'analyse. Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser. Vous pouvez analyser votre ordinateur à tout moment en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Vous pouvez aussi les planifier pour être exécutées régulièrement ou lorsque votre système est inactif afin de ne pas interférer dans votre travail.

7.2.1. Tâches d'analyse

BitDefender comporte plusieurs tâches créées par défaut qui permettent de traiter les problèmes de sécurité les plus courants. Vous pouvez aussi créer vos propres tâches d'analyse personnalisées. Chaque tâche comporte une fenêtre **Propriétés** vous permettant de configurer la tâche et d'afficher les résultats de l'analyse. Pour plus d'informations, reportez-vous à “Configuration des tâches d'analyse” (p. 54).

Il y a trois catégories de tâches d'analyse :
• **Tâches système** - contiennent une liste des tâches système par défaut. Les tâches suivantes sont disponibles :

Tâche d'analyse par défaut	Description
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malicieux menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse complète du système	Analyse l'ensemble du système, mis à part les archives. La configuration par défaut permet d'analyser tous les types de codes malicieux menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse rapide du système	Analyse les répertoires Windows,Program Files et All Users). La configuration par défaut permet d'analyser tous les types de codes malicieux, à l'exception des rootkits, mais ne permet pas d'analyser la mémoire, les registres et les cookies.



Note
Sachant que les tâches d'Analyse approfondie du système et d'Analyse complète du système analysent l'intégralité du système, l'analyse peut prendre un certain temps. C'est pourquoi nous vous recommandons d'exécuter ces tâches en priorité faible ou, encore mieux, lorsque votre système est inactif.

- **Tâches prédéfinies** - contiennent les tâches prédéfinies par l'utilisateur. Une tâche Mes documents vous est proposée. Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel : Mes documents, Bureau et Démarrage. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.
- **Tâches diverses** - contiennent une liste de tâches diverses. Ces tâches font référence à des modes d'analyse différents qui ne peuvent pas être lancés depuis cette fenêtre. Vous pouvez uniquement modifier leurs paramètres et voir le rapport d'analyse.

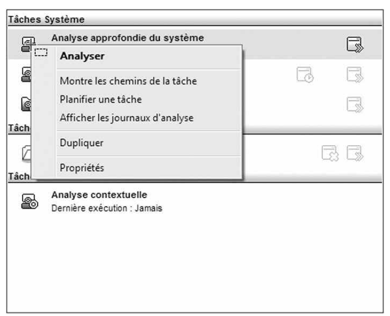
Trois boutons sont disponibles à la droite de chaque tâche :
- **Planifier** - indique que la tâche sélectionnée est planifiée pour être exécutée ultérieurement. Cliquez sur ce bouton pour ouvrir la fenêtre **Propriétés** et l'onglet **Planificateur** permettant d'afficher la tâche planifiée et de la modifier.
- **Supprimer** - supprime la tâche sélectionnée



Note
Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

- Analyser - lance la tâche sélectionnée, démarrant ainsi une analyse immédiate.

7.2.2. Utilisation du menu de raccourcis



Menu de raccourci

Un menu de raccourci est également disponible pour chaque tâche. Utilisez le "clic-droit" sur la tâche sélectionnée pour y accéder.

Les commandes suivantes sont disponibles dans le menu de raccourcis :
- **Lancer l'analyse** - démarre immédiatement la tâche d'analyse choisie.
- **Chemins** - ouvre la fenêtre Propriétés et l'onglet Chemins permettant de modifier la cible à analyser de la tâche sélectionnée.
- **Planifier** - ouvre la fenêtre Propriétés et l'onglet Planificateur permettant de planifier la tâche sélectionnée.
- **Journaux** - ouvre la fenêtre Propriétés, l'onglet Journaux, où vous pouvez consulter les rapports générés après l'exécution des tâches sélectionnées.
- **Cloner** - reproduit la tâche sélectionnée.



Note
Très utile lors de la création de nouvelles tâches car cette fonction vous permet aussi d'en modifier les propriétés si besoin.

- **Effacer** - efface la tâche sélectionnée.



Note
Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

- **Ouvrir** - ouvre la fenêtre Propriétés et l'onglet Vue d'ensemble permettant de modifier les paramètres de la tâche sélectionnée.



Note
Seules les options des onglets Propriétés et Journaux sont disponibles dans la catégorie Tâches diverses.

7.2.3. Création de tâches d'analyse

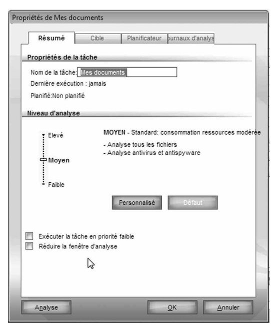
Pour créer une tâche d'analyse, utilisez l'une des méthodes suivantes :
- **Dupliquez une tâche existante,** renommez-la et effectuez les modifications nécessaires dans la fenêtre Propriétés.
- **Nouvelle tâche :** permet de créer une nouvelle tâche et de la configurer.

7.2.4. Configuration des tâches d'analyse

Chaque tâche d'analyse dispose de sa propre fenêtre de Propriétés, dans laquelle vous pouvez configurer les options d'analyse, définir les éléments à analyser, programmer une tâche ou voir le rapport. Pour ouvrir cette fenêtre, cliquez sur le bouton **Ouvrir**, situé à droite de la tâche (ou cliquez sur la tâche avec le bouton droit de la souris puis sélectionnez **Ouvrir**.



Note
Pour plus d'informations sur l'affichage des journaux et sur l'onglet Journaux, reportez-vous à “Afficher les journaux d'analyse” (p. 65).



Configuration des paramètres d'analyse

Pour configurer les options d'analyse d'une tâche d'analyse spécifique, faites un clic droit et sélectionnez Ouvrir. La fenêtre suivante apparaît :

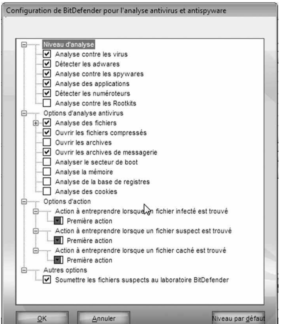
Vue d'ensemble
Vous trouverez dans cette rubrique les informations concernant les tâches (nom, dernière analyse, planification) et aurez la possibilité de définir les paramètres d'analyse.

Sélection du niveau d'analyse
Vous pouvez facilement configurer les paramètres d'analyse en sélectionnant le niveau d'analyse. Déplacez le curseur sur l'échelle pour définir le niveau d'analyse approprié.
Il y a 3 niveaux d'analyse :

Tâche d'analyse par défaut	Description
Basse	Offre un niveau de détection correct. La consommation de ressources est faible. Seuls les programmes sont scannés pour détecter les virus. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Offre un niveau de détection efficace. La consommation de ressources système est modérée.
Moyenne	Tous les fichiers sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Offre un niveau de détection élevé. La consommation de ressources système est élevée.
Agressif	Tous les fichiers et les fichiers archives sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Une série d'options générales de paramétrage de l'analyse sont également disponibles :

Option	Description
Exécuter la tâche d'analyse avec une priorité basse	Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie. Réduit la fenêtre d'analyse dans la barre d'état système. Double-cliquez sur l'icône de BitDefender pour l'ouvrir.
Réduire la fenêtre d'analyse au démarrage dans la barre d'état système	Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur Analyser.
Agressif	Tous les fichiers et les fichiers archives sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, BitDefender utilise un moteur d'analyse heuristique. Une série d'options générales de paramétrage de l'analyse sont également disponibles :

Personnalisation du niveau d'analyse
Les utilisateurs avancés peuvent utiliser les paramètres d'analyse proposés par BitDefender. Le moteur d'analyse peut être configuré pour analyser uniquement des extensions de fichiers spécifiques, pour rechercher des menaces de codes malveillants spécifiques ou pour passer les archives. Cela peut permettre de réduire considérablement la durée d'une analyse et d'améliorer la réactivité de votre ordinateur lors de l'analyse. Cliquez sur **Personnalisé** pour définir vos propres options d'analyse. Une nouvelle fenêtre est alors affichée.



Options d'analyse

Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows. Cliquez sur la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.
Les options d'analyse sont groupées en quatre catégories :
- **Niveau d'analyse**
- **Options d'analyse des virus**
- **Options d'action**
- **Autres options**
- Spécifiez le type de codes malicieux que vous souhaitez que BitDefender analyse en sélectionnant les options correspondantes dans la catégorie **Niveau d'analyse.**

Les options suivantes sont disponibles :

Option	Description
Analyse antivirus	Analyse les virus connus. BitDefender détecte également les corps de virus incomplets, permettant ainsi d'écarter toute menace potentielle pouvant affecter la sécurité de votre système.
Analyse anti-adwares	Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée.
Analyse anti-spywares	Recherche les menaces de type spyware. Les fichiers détectés sont traités en tant que fichiers infectés.
Analyse des applications	Analyse les applications (fichiers .exe et .dll). infectés. Un logiciel incluant des composants de type numéroteur peut ne plus fonctionner si cette option est activée.
Analyse anti-dialers	Analyse les applications qui appellent des numéros surtaxés. Les fichiers détectés sont traités en tant que fichiers
Analyse anti-rootkits	Analyse les objets cachés (fichiers, entrées registres, processus), plus connus sous le nom de rootkits.

- Spécifiez le type d'objets à analyser (archives, emails et autres) ainsi que d'autres options. Cela se fait par la sélection de certaines options dans la catégorie **Options d'analyse des virus.**

Les options suivantes sont disponibles :

Option	Description
Analyse de tous les fichiers	Tous les fichiers seront analysés à l'accès, quel que soit leur type.
Analyse des extensions à risques seulement	Seuls les fichiers avec les extensions suivantes seront analysés : exe ; bat ; com ; dll ; ocx ; scr ; bin ; dat ; 386 ; vxd ; sys ; wdm ; cla ; lass ; ovl ; ole ; exe ; hlp ; doc ;dot ; xls ; ppt ; wbk ; wiz ; pot ; ppa ; xla ; xlt ; vbs ; vbe ;mdb ; rtf ; htm ; hta ; html ; xml ; xtp ; php ; asp ; js ; shs ; chm ; lnk ; pif ; prc ; url ; smm ; pdf ; msi ; ini ; csc ; cmd ;bas ; eml et nws.
Analyse des extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par " ;".
Ouvrir les fichiers compressés	Analyser les fichiers compressés.
Ouvrir les fichiers archives	Analyser l'intérieur des fichiers archives.fichiers
Ouvrir les archives de messagerie	Analyser dans les archives de messagerie
Analyser les secteurs de boot	Analyser les secteurs de boot du système
Analyse de la mémoire	Analyser la mémoire pour détecter les virus et les autres malwares.
Analyse de la base de registre	Analyse les entrées du Régistre.
Analyse des cookies	Analyse les cookies.

- Spécifiez les actions à mener sur les fichiers infectés, suspects ou cachés détectés dans la catégorie Options d'action. Vous pouvez spécifier une action différente pour chaque catégorie.

- Sélectionnez l'action à mener sur les fichiers infectés détectés. Les options suivantes sont disponibles :

Aucune : Aucune action ne sera prise sur les fichiers infectés. Ceux-ci vont apparaître dans le fichier des rapports.
Désinfecter : Pour désinfecter un fichier infecté.
Supprimer : Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer en quarantaine : Déplace les fichiers infectés dans la zone de quarantaine.

- Sélectionnez l'action à mener sur les fichiers suspects détectés. Les options suivantes sont disponibles :

Aucune : Aucune action ne sera menée sur les fichiers suspects. Ces fichiers apparaîtront dans le fichier d'état.
Supprimer : Supprime immédiatement les fichiers suspects, sans avertissement.
Déplacer en quarantaine : Déplace les fichiers suspects dans la zone de quarantaine.



Note
Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Nous vous recommandons de les envoyer au laboratoire BitDefender.

• Sélectionnez l'action à mener sur les objets cachés (rootkits) détectés. Les options suivantes sont disponibles :

Aucune : Aucune action ne sera menée sur les fichiers cachés. Ces fichiers apparaîtront dans le fichier d'état.
Déplacer en quarantaine : Déplace les fichiers cachés dans la zone de quarantaine.
Rendre visible : Affiche les fichiers cachés pour vous permettre de les visualiser.



Note
Si vous choisissez d'ignorer les fichiers détectés ou si l'action sélectionnée échoue, vous devrez sélectionner une action dans l'assistant d'analyse.

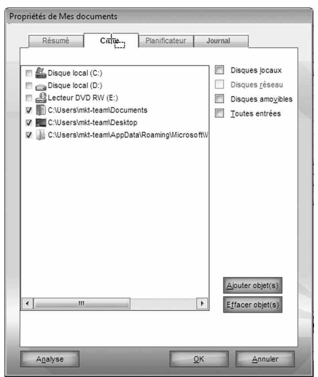
• Pour être invité à envoyer tous les fichier suspects au laboratoire BitDefender une fois le processus d'analyse terminé, cliquez sur Soumettre les fichiers suspects au laboratoire BitDefender dans la catégorie Autres options.
Si vous cliquez sur **Défaut** vous chargerez les paramètres par défaut. Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

Définition de la cible à analyser



Note
Vous ne pouvez pas modifier la cible à analyser des tâches d'analyse à partir des catégories Tâches Système et Tâches Diverses. La fenêtre Propriétés de ces tâches ne comporte pas cet onglet.

Pour définir la cible à analyser d'une tâche d'analyse spécifique, faites un clic droit sur la tâche et sélectionnez Chemins. La fenêtre suivante apparaît :



Analyser la cible

Vous pouvez afficher la liste des lecteurs locaux, réseau ou amovibles, ainsi que les fichiers ou dossiers ajoutés précédemment, le cas échéant. Tous les éléments cochés seront analysés lors de l'exécution de la tâche.
Cette partie contient les boutons suivants :
• **Ajouter éléments** - ouvre une fenêtre permettant de sélectionner les fichiers/dossiers que vous souhaitez analyser.



Note
Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant.

• **Supprimer éléments** - supprime les fichiers/dossiers précédemment sélectionnés de la liste des objets à analyser.



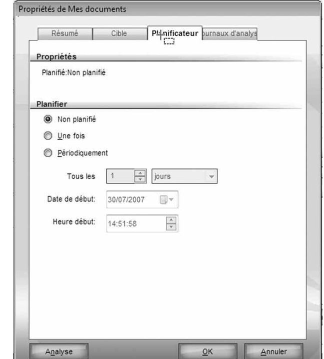
Note
Seuls les fichiers/dossiers rajoutés après peuvent être effacés, pas ceux automatiquement "proposés" par BitDefender.

Ces options permettent une sélection rapide des cibles d'analyses.
• **Disques locaux** - pour analyser les disques locaux.
• **Disques réseaux** - pour analyser tous les lecteurs réseaux.
• **Disques amovibles** - pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
• **Toutes les entrées** - pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.



Note
Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case Toutes les entrées.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser.**



Planification des tâches d'analyse
Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. L'utilisateur doit pour cela créer une tâche à l'avance.
Pour afficher la planification d'une tâche spécifique ou la modifier, faites un clic droit sur la tâche et sélectionnez Planifier. La fenêtre suivante apparaît :

Planificateur
La tâche planifiée s'affiche, le cas échéant.
Quand vous programmez une tâche, vous devez choisir une des options suivantes :
• Aucune planification - lance la tâche uniquement si l'utilisateur le demande.
• Une fois - lance l'analyse une fois seulement, à un certain moment. Spécifiez la date et l'heure de démarrage dans le champ Démarrer Date/Heure.
• Si vous souhaitez que l'analyse soit répétée à intervalle régulier, cochez la case Périodiquement

• Si vous voulez que l'analyse se répète à intervalle régulier, cochez la case Périodiquement et précisez dans les champs prévus minutes/heures/jours/semaines/mois/années. Vous devez également déterminer la date de début et de fin dans le champ Date de début/Heure.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

7.2.5. Analyse des objets

Avant de lancer un processus d'analyse, assurez-vous que BitDefender est à jour dans les signatures de codes malveillants. L'analyse de votre ordinateur au moyen d'une base de données de signatures obsolète pourrait empêcher BitDefender de détecter les nouveaux codes malveillants à rechercher depuis la dernière mise à jour. Pour vérifier la date de la dernière mise à jour, cliquez sur **Mise à jour > Mise à jour dans la console des paramètres**.



Note

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes en cours d'utilisation, tout spécialement les clients de messagerie (ex : Outlook, Outlook Express ou Eudora).

Méthodes d'analyse

BitDefender permet quatre types d'analyse à la demande :

• **Analyse immédiate** - lance une tâche d'analyse depuis les tâches disponibles.
• **Analyse contextuelle** - faîtes un clic-droit sur un fichier ou répertoire et sélectionnez BitDefender Antivirus 2008.
• **Analyse par glisser-déposer** - glissez & déposez un fichier ou un répertoire sur la barre d'analyse d'activité.
• **Analyse manuelle** - utilisez l'analyse manuelle BitDefender pour sélectionner directement les fichiers ou répertoires que vous souhaitez analyser.

Analyse immédiate

Vous pouvez analyser tout ou partie de votre ordinateur en exécutant les tâches d'analyse par défaut ou vos propres tâches d'analyse. Cela s'appelle l'analyse immédiate.

Pour exécuter une tâche d'analyse, utilisez l'une des méthodes suivantes :

• Double-cliquez sur la tâche d'analyse souhaitée dans la liste.
• Cliquez sur le bouton Analyser correspondant à la tâche.
• Sélectionnez la tâche, puis cliquez sur Exécuter la tâche.

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à "Moteur d'analyse BitDefender" (p. 62).



Analyse contextuelle

Pour analyser un fichier ou un dossier sans configurer de nouvelle tâche d'analyse, vous pouvez utiliser le menu contextuel. Cela s'appelle l'analyse contextuelle.

Faîtes un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option BitDefender Antivirus 2008.

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à "Moteur d'analyse BitDefender"(p. 62).

Vous pouvez modifier les options d'analyse et voir les fichiers de rapport à partir de la fenêtre Propriétés de la tâche Analyse via le menu contextuel.

Analyse par glisser&déposer

Glissez le fichier ou répertoire que vous voulez analyser et déposez-le sur la Barre d'analyse de l'activité, comme sur l'image ci-dessous.



Glisser le fichier



Déposer le fichier

Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à "Moteur d'analyse BitDefender" (p. 62).

Analyse manuelle

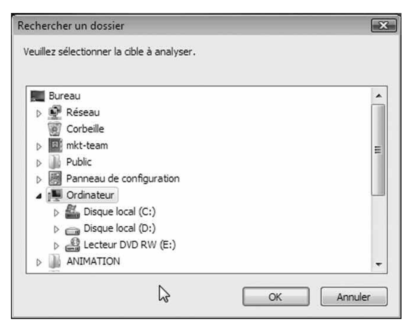
L'analyse manuelle consiste à sélectionner directement les fichiers ou répertoires que vous souhaitez analyser avec l'option d'analyse manuelle Bitdefender disponible depuis le menu Démarrer de Windows dans le groupe de programme BitDefender.



Note

L'analyse manuelle est très pratique car elle peut également être effectuée lorsque Windows est en mode sans échec.

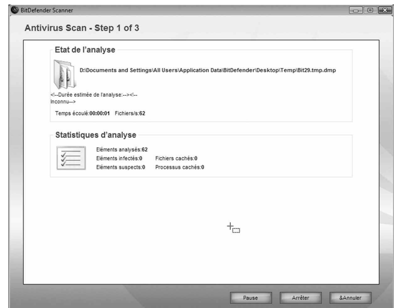
Pour sélectionner les fichiers ou répertoires que BitDefender doit analyser, suivez le chemin suivant depuis le menu Démarrer de Windows : Démarrer _ Programmes _ BitDefender 2008 _ Analyse manuelle BitDefender.
La fenêtre suivante apparaît :



Analyse manuelle
Choisissez les fichiers ou répertoires que vous souhaitez analyser et cliquez sur **OK**. Lorsque le moteur d'analyse BitDefender apparaît, l'analyse est lancée. Pour plus d'informations, reportez-vous à “Moteur d'analyse BitDefender” (p. 62).

Moteur d'analyse BitDefender
Lorsque vous lancez un processus d'analyse sur demande, le moteur d'analyse BitDefender apparaît.
Suivez cette procédure en trois étapes pour effectuer le processus d'analyse :

Étape 1 sur 3 - Analyse
BitDefender commence à analyser les objets sélectionnés.



Analyse en cours
Le statut et les statistiques de l'analyse s'affichent (vitesse d'analyse, temps écoulé, nombre d'objets analysés / infectés / suspects / cachés, etc.).



Note
L'analyse peut durer un certain temps, suivant la complexité de l'analyse.

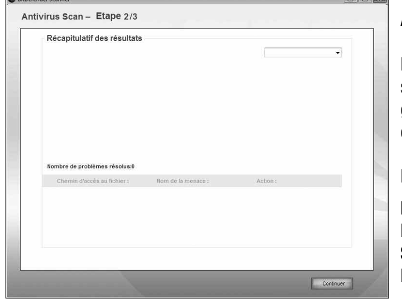
Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur Reprendre.
Vous pouvez arrêter l'analyse à tout moment en cliquant sur Arrêter et **Oui**. Vous vous retrouverez alors à la dernière étape de l'assistant.



Note
Lorsque des fichiers suspects seront détectés durant l'analyse, vous serez invité à les envoyer au laboratoire BitDefender.

Patientez jusqu'à ce que BitDefender ait terminé l'analyse.

Étape 2 sur 3 - Sélectionner des actions
Une fois l'analyse terminée, une nouvelle fenêtre apparaît affichant les résultats de l'analyse.



Actions

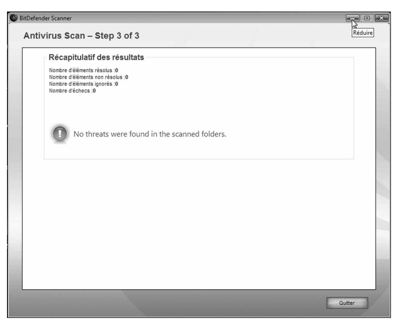
Le nombre de problèmes de sécurité affectant votre système est indiqué. Les problèmes de sécurité sont affichés en groupes. Cliquez sur "**+**" pour ouvrir un groupe ou sur "**-**" pour fermer un groupe. Vous pouvez sélectionner une action globale à mener pour chaque groupe de problèmes de sécurité ou sélectionner des actions spécifiques pour chaque problème.

Les options suivantes peuvent s'afficher dans le menu :

Ne pas mener d'action :	Aucune action ne sera menée sur les fichiers détectés.
Désinfecter :	Pour désinfecter un fichier infecté.
Supprimer :	Pour supprimer les fichiers détectés.
Démasquer :	Rend les objets cachés visibles.

Cliquez sur **Réparer** pour appliquer les actions spécifiées.

Étape 3 sur 3 - Voir les résultats
Une fois les problèmes de sécurité résolus par BitDefender, les résultats de l'analyse apparaissent dans une nouvelle fenêtre.

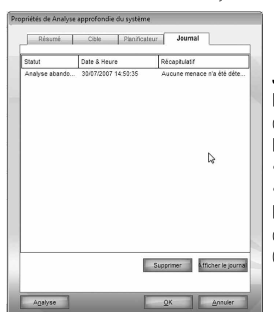


Récapitulatif
Le récapitulatif des résultats s'affiche. Le fichier rapport est sauvegardé automatiquement dans la rubrique Journaux de la fenêtre Propriétés de la tâche en question.

Avertissement
Dans le cas d'un problème de sécurité non résolu, nous vous recommandons de contacter le support BitDefender sur le site www.bitdefender.com.

7.2.6. Afficher les journaux d'analyse

Pour afficher les résultats de l'analyse une fois la tâche exécutée, faites un clic droit sur la tâche et sélectionnez Journaux. La fenêtre suivante apparaît :



Journaux d'analyse
Dans cette partie vous visualisez le rapport généré à chaque fois qu'une tâche est exécutée. Chaque fichier dispose d'informations sur son état (ok/infecté), la date et la durée de l'analyse et un récapitulatif.
Deux boutons sont disponibles :
- **Afficher** - ouvre le fichier rapport sélectionné.
- **Effacer** - supprime le fichier rapport sélectionné.

Pour effacer ou visualiser un fichier, vous pouvez également faire un "clic-droit" sur le fichier et choisir l'option correspondante.
Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

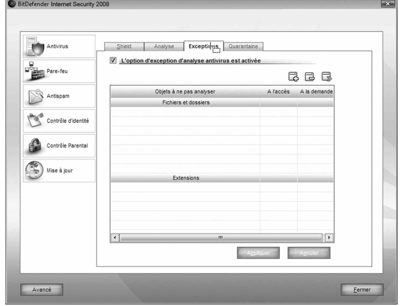
7.3. Objets exclus de l'analyse

Il peut arriver de devoir exclure certains fichiers de l'analyse. Par exemple, il peut être utile d'exclure un fichier test EICAR d'une analyse à l'accès ou des fichiers .avi d'une analyse sur demande. BitDefender vous permet d'exclure des objets d'une analyse à l'accès ou d'une analyse sur demande ou des deux. Cette fonction permet de réduire la durée d'une analyse et d'éviter d'interférer dans votre travail.
Deux types d'objet peuvent être exclus d'une analyse :
- **Chemins** - un fichier ou un dossier (avec tous les objets qu'il contient) indiqué par un chemin spécifique ;
- **Extensions** - tous les fichiers ayant une extension spécifique.



Note
Les objets exclus d'une analyse à l'accès ne sont pas analysés, que ce soit vous-même ou une application qui y accédiez.

Pour afficher et gérer les objets exclus de l'analyse, cliquez sur Antivirus > Exceptions dans la console des paramètres. La fenêtre suivante apparaît :



Exceptions
Les objets (fichiers, dossiers, extensions) exclus de l'analyse s'affichent. Il est indiqué pour chaque objet si celui-ci est exclus d'une analyse à l'accès, d'une analyse sur demande ou des deux.



Note
Les exceptions spécifiées ici ne s'appliquent PAS à l'analyse contextuelle.

Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.
Pour editer un objet de la liste, sélectionnez le et cliquez sur le bouton **Editer**. Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **OK**.

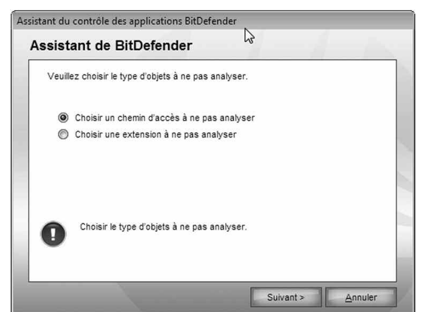


Note
Vous pouvez aussi faire un clic droit sur un objet et utiliser les options du menu de raccourcis pour le modifier ou le supprimer.

Vous pouvez cliquer sur **Annuler** pour revenir aux modifications effectuées dans le tableau des règles, à condition que vous ne les ayez pas enregistrées en cliquant sur **Appliquer**.

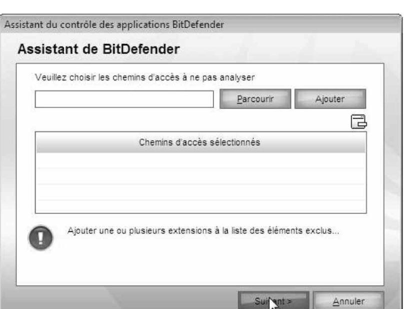
7.3.1. Exclusion des chemins de l'analyse

Pour exclure des chemins de l'analyse, cliquez sur le bouton **Ajouter**. Vous serez guidé tout au long du processus d'exclusion par l'assistant de configuration qui apparaîtra.



Étape 1 sur 3 - Sélectionner le type d'objet

Type d'objet
Sélectionnez l'option d'exclusion d'un chemin de l'analyse.
Cliquez sur **Suivant**.



Cliquez sur **Suivant**.

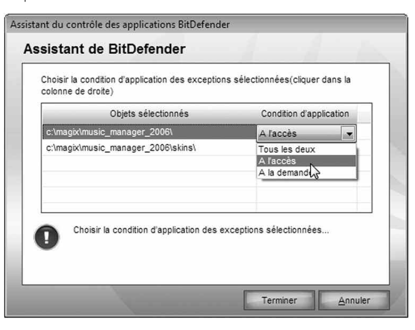
Étape 2 sur 3 - Spécifier les chemins à exclure
Chemins à exclure
Pour spécifier les chemins à exclure de l'analyse, utilisez l'une des méthodes suivantes :

- Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **Ajouter**.
- Saisissez le chemin à exclure de l'analyse dans la zone de texte, puis cliquez sur Ajouter.



Note
Si le chemin indiqué n'existe pas, un message d'erreur apparaît. Cliquez sur OK et vérifiez la validité du chemin.

Les chemins apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez. Pour effacer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**.



Étape 3 sur 3 - Sélectionner le type d'analyse

Type d'analyse
Un tableau contenant les chemins à exclure de l'analyse et le type d'analyse dont ils sont exclus est affiché. Par défaut, les chemins sélectionnés sont exclus à la fois de l'analyse à l'accès et de l'analyse sur demande. Pour modifier quand appliquer l'exception, cliquez sur la colonne de droite et sélectionnez l'option souhaitée dans la liste.

Cliquez sur **Terminer.**

N'oubliez pas de cliquer sur **Appliquer** pour enregistrer vos modifications.

7.3.2. Exclusion des extensions de l'analyse



Pour exclure des extensions de l'analyse, cliquez sur le bouton **Ajouter**. Vous serez guidé tout au long du processus d'exclusion par l'assistant de configuration qui apparaîtra.

Étape 1 sur 3 - Sélectionner le type d'objet

Type d'objet
Sélectionnez l'option d'exclusion d'une extension de l'analyse.
Cliquez sur **Suivant**.

Étape 2 sur 3 - Spécifier les extensions à exclure



Extensions à exclure

Pour spécifier les extensions à exclure de l'analyse, utilisez l'une des méthodes suivantes :

- Sélectionnez dans le menu l'extension que vous souhaitez exclure de l'analyse, puis cliquez sur **Ajouter**.



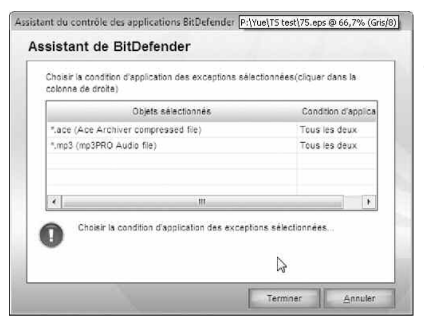
Note

Le menu contient la liste de toutes les extensions enregistrées dans votre système. Lorsque vous sélectionnez une extension, sa description s'affiche si elle est disponible.

- Saisissez l'extension à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**. Les extensions apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez. Pour effacer un objet de la liste, sélectionnez le et cliquez sur le bouton **Effacer**.

Cliquez sur **Suivant**.

Étape 3 sur 3 - Sélectionner le type d'analyse



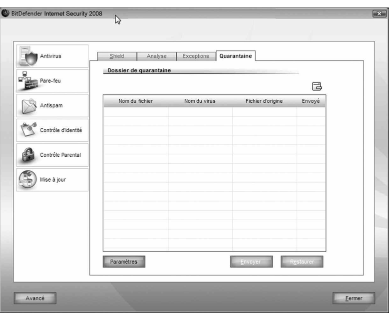
Type d'analyse

Un tableau s'affiche contenant les extensions devant être exclues de l'analyse et le type d'analyse dont elles sont exclues. Par défaut, les extensions sélectionnées sont exclues à la fois de l'analyse à l'accès et de l'analyse sur demande. Pour modifier quand appliquer l'exception, cliquez sur la colonne de droite et sélectionnez l'option souhaitée dans la liste.

Cliquez sur **Terminer**.

N'oubliez pas de cliquer sur **Appliquer** pour enregistrer vos modifications.

7.4. Zone de quarantaine



Quarantaine

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender. Pour afficher et gérer les fichiers en quarantaine et pour configurer les paramètres de la quarantaine, cliquez sur **Antivirus > Quarantaine** dans la console des paramètres.

7.4.1. Gérer les fichiers en quarantaine

Comme vous le constaterez, la rubrique **Quarantaine** contient une liste de tous les fichiers qui ont été isolés jusque là. Chaque fichier intègre son nom, sa taille, sa date d'isolation et sa date de soumission.



Note

Lorsque le virus est en quarantaine, il ne peut faire aucun dégât puisqu'il ne peut être exécuté ou lu.

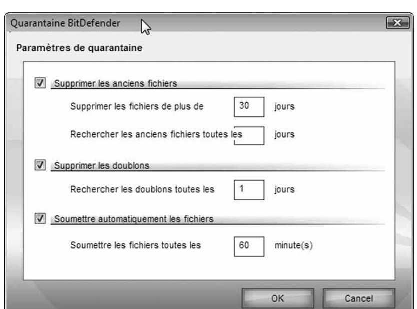
Pour effacer un fichier sélectionné dans la zone de quarantaine, cliquez sur le bouton **Déplacer**. Si vous voulez restaurez un fichier sélectionné dans son emplacement d'origine, cliquez sur Restaurer.

Vous pouvez envoyer un fichier depuis la quarantaine aux BitDefender Labs en cliquant sur **Envoyer**.

Menu contextuel. Le menu contextuel qui vous est proposé vous permet de gérer facilement les fichiers en quarantaine. Les options disponibles sont les mêmes que celles mentionnées précédemment. Vous pouvez aussi sélectionner **Actualiser** pour rafraîchir la zone de quarantaine.

7.4.2. Configuration des paramètres de la quarantaine

Pour configurer les paramètres de la quarantaine, cliquez sur **Paramètres**. Une nouvelle fenêtre s'affiche.



Configuration de la zone de quarantaine

En utilisant les paramètres de la quarantaine, vous pouvez configurer BitDefender pour exécuter automatiquement les actions suivantes :

Supprimer les anciens fichiers. Pour supprimer automatiquement les anciens fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier après combien de jours les fichiers en quarantaine doivent être supprimés et la fréquence à laquelle BitDefender doit rechercher les anciens fichiers.



Note

Par défaut, BitDefender recherche les anciens fichiers chaque jour et supprime les fichiers de plus de 10 jours.

Supprimer les doublons. Pour supprimer automatiquement les doublons de fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier le nombre de jours entre deux recherches consécutives de doublons.

Soumettre automatiquement les fichiers. Pour soumettre automatiquement les fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier la fréquence à laquelle soumettre les fichiers.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

8. Pare-feu

Le pare-feu protège votre ordinateur contre les tentatives de connexion entrantes et sortantes non autorisées.
On peut le comparer à un gardien – il gardera un œil sur votre connexion Internet et conservera une trace des programmes autorisés à y accéder et de ceux qui doivent être bloqués.



Note
Un Pare-feu est essentiel si vous possédez une connexion de type ADSL.

En mode "camouflé" votre ordinateur est "invisible" pour les pirates. Le module Pare-feu est capable de détecter automatiquement les "scans de port" et de protéger votre ordinateur. (Les scans de port servent a détecter les points d'accès disponibles sur une machine et précèdent généralement une attaque.)
La rubrique **Pare-feu** de ce Manuel d'utilisation contient les thèmes suivants :

- Aperçu du pare-feu
- Etat du Pare-feu
- Protection du trafic
- Paramètres avancés
- Activité du Pare-feu
- Zones réseau

8.1. Aperçu du Pare-feu

Le Pare-feu de BitDefender protège efficacement votre réseau/vos connexions Internet sans qu'il soit nécessaire de le configurer. Que vous soyez directement connecté à Internet, à un réseau unique ou à plusieurs réseaux (réseau Ethernet, sans fil, VPN ou autre), fiables ou non, votre Pare-feu s'auto-configure pour s'adapter à la situation.
Par défaut, BitDefender détecte automatiquement les configurations réseau de votre ordinateur et crée un profil de Pare-feu standard approprié. Il ajoute également au profil les réseaux détectés en tant que zones réseau fiables ou non fiables, selon leur configuration.

8.1.1. Que sont les profils de Pare-feu ?

Un profil de Pare-feu est un ensemble de règles qui contrôle l'accès Internet/réseau des applications.
En fonction de la configuration réseau de votre ordinateur, BitDefender crée automatiquement un type de profil spécifique. Le profil standard créé contient des règles d'accès réseau ou des règles élémentaires d'accès Internet requises par les applications du système et les composants BitDefender.



Note
Un profil de Pare-feu unique est créé, indépendamment du nombre de réseaux auxquels vous êtes connecté.

Il existe trois types de profils standards :

Connexion directe : Contient les règles élémentaires d'accès Internet recommandées pour une configuration réseau autorisant l'accès direct à Internet. Ces règles n'autorisent pas les utilisateurs du réseau à accéder à votre ordinateur et ne vous autorisent pas non plus à naviguer dans le réseau.

Non fiable : Contient les règles d'accès réseau recommandées pour une configuration réseau associée à un réseau non fiable. Ces règles vous autorisent à naviguer dans le réseau, mais empêchent les autres utilisateurs du réseau d'accéder à votre ordinateur.

Fiable : Contient les règles d'accès réseau recommandées pour une configuration réseau associée à un réseau fiable. Il n'y a aucune restriction imposée sur l'accès réseau. Cela signifie que vous avez accès aux volumes partagés, aux imprimantes réseau et à d'autres ressources du réseau. Cela signifie aussi que les utilisateurs du réseau peuvent se connecter à votre ordinateur et accéder à vos partages.

Lorsque les applications tentent de se connecter à Internet, les règles appropriées sont ajoutées au profil. Vous pouvez choisir d'autoriser ou de refuser par défaut l'accès Internet aux applications pour lesquelles les règles n'ont pas été configurées ou de n'autoriser par défaut que les applications en liste blanche et de donner votre autorisation pour les autres.



Note
Pour spécifier la politique d'accès des applications tentant de se connecter à Internet pour la première fois, rendez vous dans la section État et définissez le niveau de protection souhaité. Pour modifier le profil existant, rendez vous dans la section Trafic et cliquez sur Éditer le profil.

8.1.2. Que sont les zones réseau ?

Une zone réseau représente un ordinateur dans un réseau ou un réseau entier complètement isolé de votre ordinateur ou, au contraire, capable de détecter votre ordinateur et de s'y connecter.
Concrètement, une zone est une adresse IP ou un ensemble d'adresses IP dont l'accès à votre ordinateur est autorisé ou refusé.
Par défaut, BitDefender ajoute automatiquement des zones pour les configurations réseau spécifiques. Les zones sont ajoutées en créant des règles d'accès réseau appropriées, applicables à un réseau entier, dans le profil actuel. Il existe deux types de zone :

Fiable : Les ordinateurs d'une zone fiable peuvent se connecter à votre ordinateur et vous pouvez vous connecter à eux. Toutes les tentatives de connexion provenant d'une zone de ce type et toutes celles provenant de votre ordinateur vers ce type de zone sont autorisées. Si un réseau est ajouté en tant que zone fiable, cela signifie que vous avez un accès illimité aux volumes partagés, aux imprimantes et à d'autres ressources de ce réseau. De plus, les utilisateurs du réseau peuvent se connecter à votre ordinateur et accéder à vos partages.

Non fiable : Les ordinateurs d'une zone non fiable n'ont pas la possibilité de se connecter à votre ordinateur et vous ne pouvez pas non plus vous connecter à eux. Toutes les tentatives de connexion provenant d'une zone de ce type et toutes celles provenant de votre ordinateur vers ce type de zone sont bloquées. Comme tout le trafic ICMP est refusé et que le mode furtif est activé, votre ordinateur est quasiment invisible pour les ordinateurs de cette zone.



Note
Pour modifier une zone, accédez à la section Zones. Pour modifier la règle correspondant à une zone spécifique, accédez à la section Trafic et cliquez sur Éditer le profil.

8.1.3. Fonctionnement du Pare-feu

Lors de la réinitialisation du système une fois l'installation effectuée, BitDefender détecte automatiquement votre configuration réseau, crée un profil standard approprié et ajoute une zone en fonction du réseau détecté.



Note
Si vous êtes directement connecté à Internet, aucune zone réseau ne sera créée pour la configuration réseau correspondante. Si vous êtes connecté à plusieurs réseaux, les zones seront ajoutées en fonction des différents réseaux.

Chaque fois que votre configuration réseau est modifiée, que ce soit lorsque vous vous connectez à un autre réseau ou si vous désactivez une connexion réseau, un nouveau profil de Pare-feu est créé et les zones réseau sont modifiées en conséquence.

Lorsqu'un nouveau profil de Pare-feu est créé, l'ancien profil est sauvegardé pour pouvoir être à nouveau chargé lors de votre prochaine utilisation de la configuration réseau correspondante.

BitDefender se configure en fonction de la configuration réseau. Voici comment le Pare-feu de BitDefender est configuré par défaut :

- Si vous êtes directement connecté à Internet, indépendamment du fait que vous soyez également connecté à d'autres réseaux, un profil de connexion directe est créé. Sinon, BitDefender crée un profil de Pare-feu non fiable.



Note
Pour une question de sécurité, les profils fiables ne sont pas créés par défaut. Pour créer un profil fiable, vous devez réinitialiser le profil existant. Pour plus d'informations, reportez-vous à “Réinitialisation des profils” (p. !! 48).

- Les zones sont ajoutées en fonction de la configuration réseau.

Fiable : **IP privée sans passerelle** - L'ordinateur fait partie d'un réseau local (LAN) et n'est pas connecté à Internet (par exemple, un réseau domestique créé pour permettre aux différents membres d'une même famille de partager des fichiers, des imprimantes ou d'autres ressources).
IP privée avec contrôleur de domaine détecté - L'ordinateur fait partie d'un réseau LAN et est connecté à un domaine (par exemple, un réseau de bureau permettant aux utilisateurs de partager des fichiers ou d'autres ressources d'un domaine). Un domaine implique l'existence d'un ensemble de politiques auxquelles les ordinateurs des différents utilisateurs se conforment.

Non fiable : **Sans fil ouvert (non sécurisé)** - L'ordinateur fait partie d'un réseau local sans fil (WLAN). (par exemple, si vous accédez à Internet via un point d'accès libre dans un lieu public).

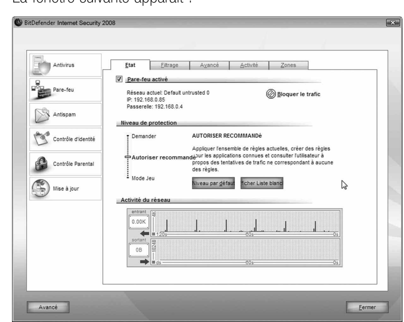


Note
Certaines configurations réseau ne requièrent pas la création de zones, telles que :
• IP publique (routable) - L'ordinateur est directement connecté à Internet.
• IP privée avec passerelle, mais aucun contrôleur de domaine détecté - L'ordinateur fait partie d'un réseau LAN, sans faire également partie d'un domaine, et se connecte à Internet via une passerelle (par exemple, un réseau scolaire permettant aux utilisateurs de partager des fichiers ou d'autres ressources).

- Le mode furtif est activé.
- Les connexions VPN (réseau privé) et à distance sont autorisées.
- Le partage des connexions Internet n'est pas autorisé pour les zones non validées.
- Alors que les applications en liste blanche ont un accès automatiquement autorisé, les autres applications requièrent votre autorisation à leur première tentative de connexion.

8.2. Etat du Pare-feu

Pour configurer la protection du Pare-feu , cliquez sur **Pare-feu > État** dans la console des paramètres.
La fenêtre suivante apparaît :



Etat du Pare-feu

Dans cette partie, vous pouvez activer / désactiver le Pare-feu, bloquer tout le trafic réseau/internet et définir le comportement par défaut sur les nouveaux évènements.



Important
Pour être protégé contre les attaques Internet, laissez le Pare-feu activé.

Pour bloquer l'ensemble du trafic réseau/Internet, cliquez sur **Bloquer le trafic**, puis sur Oui pour confirmer votre décision. Cela permettra d'isoler votre ordinateur de tous les autres ordinateurs en réseau.

Pour débloquer le trafic ultérieurement, il suffit de cliquer sur **Débloquer le trafic.**
Dans la partie inférieure de cette rubrique, vous pouvez voir les statistiques BitDefender concernant le trafic entrant et sortant. Le graphique affiche le volume du trafic Internet sur les deux dernières minutes.



Note
Le graphique apparaît même si le Pare-feu est désactivé.

8.2.1. Configuration du niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.
Il existe trois niveaux de protection :

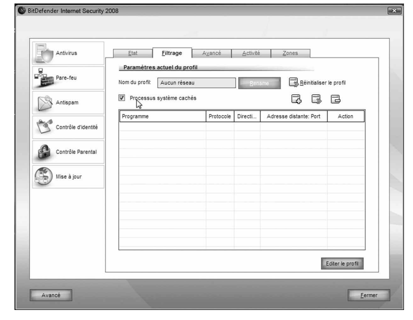
Mode jeu : Applique les règles en cours et autorise toutes les tentatives de connexion ne correspondant à aucune des règles en cours, sans interroger l'utilisateur. Cette politique est fortement déconseillée mais peut être utile à des administrateurs réseaux ou aux joueurs.

A**utoriser :** Applique les règles en cours et autorise toutes les tentatives de connexions sortantes des programmes reconnus comme légitimes (en liste blanche) par BitDefender, sans interroger. Pour les autres tentatives de connexion, BitDefender vous demandera votre autorisation. Les règles de trafic s'affichent dans la section Trafic au fur et à mesure qu'elles sont créées. Les programmes répertoriés dans la liste blanche sont les plus utilisés au niveau mondial. (Navigateurs Internet, lecteurs multimédias, programmes de partage d'applications et de fichiers etc.) Si vous voulez voir la liste des programmes en liste blanche, cliquez sur **Liste blanche**.

Demander : Applique les règles en cours et vous interroge sur les tentatives de connexion ne correspondant pas à celles en cours. Cliquez sur **Niveau par défaut** pour régler le niveau par défaut (Autoriser).

8.3. Contrôle du trafic

Pour gérer les règles du pare-feu du profil en cours, cliquez sur **Pare-feu > Trafic** dans la console des paramètres. La fenêtre suivante apparaît :

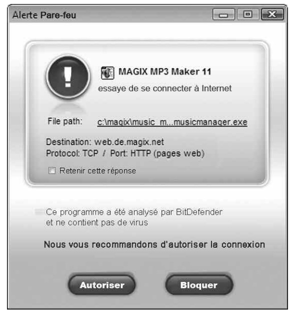


Contrôle du trafic

Dans cette partie, spécifiez quelles connexions entrantes ou sortantes sont à autoriser/interdire en définissant des règles spécifiques pour les protocoles, ports, applications et/ou les adresses distantes. Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle).

8.3.1. Ajouter des règles automatiquement

Avec le Pare-feu activé, BitDefender vous demandera votre permission chaque fois qu'une connexion Internet sera établie :



Vous pouvez voir l'application qui essaie d'accéder à Internet, le chemin au fichier d'application, la destination, le protocole utilisé et le port sur lequel l'application tente de se connecter.
Cliquez sur **Autoriser** pour autoriser l'ensemble du trafic (entrant et sortant) généré par cette application depuis l'ordinateur hôte local vers toute destination via le protocole IP respectif et sur tous les ports. Si vous cliquez sur **Bloquer**, l'application se verra refuser l'accès Internet via le protocole IP respectif.

En fonction de votre réponse, une règle sera créée, appliquée et listée dans le tableau. À la prochaine tentative de connexion de l'application, cette règle sera appliquée par défaut.

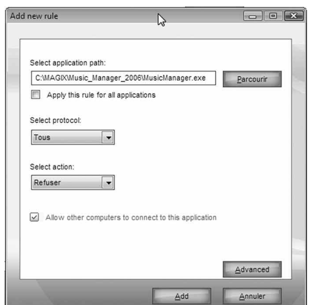
Alerte Pare-feu



Important
Autorisez les tentatives de connexion entrantes provenant d'adresses IP ou de domaines dont vous êtes sûrs.

8.3.2. Ajouter des règles manuellement

Cliquez sur le bouton **Ajouter une règle** et choisissez les paramètres de cette règle. La fenêtre suivante apparaît :



Ajouter une règle

Pour ajouter une nouvelle règle de pare-feu, suivez ces étapes :

1. Sélectionnez l'application pour laquelle la nouvelle règle de pare-feu doit être créée.
Pour sélectionner une application, cliquez sur **Parcourir**, localisez-la, puis cliquez sur **OK**.

Si vous souhaitez créer une règle pour toutes les applications, cochez simplement **Appliquer** cette règle à toutes les applications.

2. Sélectionnez le protocole auquel la règle doit s'appliquer.

Une liste avec les protocoles les plus courants est disponible pour vous aider à sélectionner un protocole spécifique. Sélectionnez le protocole désiré (sur lequel la règle s'appliquera) depuis le menu déroulant correspondant ou sélectionnez Tous pour sélectionner tous les protocoles.

Le tableau ci-dessous affiche la liste des protocoles pouvant être sélectionnés, ainsi qu'une courte description de chacun :

Option	Description
ICMP	ICMP est le terme court pour Internet Control Message Protocol – c'est une extension de Internet Protocol (IP). ICMP supporte des paquets contenant des erreurs, contrôles, et messages d'informations. La commande PING, par exemple, utilise ICMP pour tester une connexion Internet.
TCP	Transmission Control Protocol - TCP permet à deux ordinateurs d'établir une connexion et d'échanger des flux de données. TCP garantit la livraison des données et garantit également que les paquets seront livrés dans le même ordre que celui d'envoi.
UDP	User Datagram Protocol - UDP est un transport basé sur IP conçu pour de haute performance. Les jeux et des applications vidéo utilisent souvent UDP.

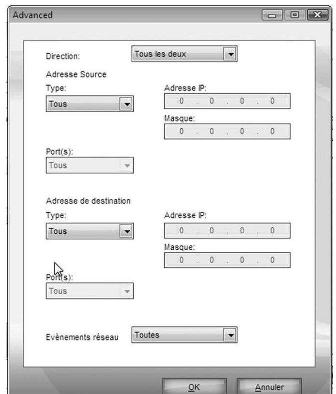
3. Sélectionnez l'action de la règle dans le menu correspondant.

Autoriser : L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.

Interdire : L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées.

4. Si le protocole précédemment sélectionné est un protocole TCP ou UDP, vous pouvez spécifier si la règle doit s'appliquer à l'application lorsqu'elle agit en tant que serveur ou pas.
Cochez **Autoriser les autres ordinateurs à se connecter à cette application** pour appliquer cette action à tous les événements réseau. Vous autoriserez ou refuserez implicitement le droit de cette application à ouvrir des ports.
Si vous souhaitez uniquement appliquer cette action au trafic pour le protocole UDP et au trafic et connexions pour le protocole TCP, décochez la case correspondante.

Pour configurer des paramètres plus avancés pour la règle, cliquez sur **Avancé**. Une nouvelle fenêtre s'affiche.



Paramètres de règle avancés

Vous pouvez configurer les options suivantes :

• Direction - sélectionne la direction du trafic.

Sortant :	La règle s'applique seulement pour le trafic sortant.
Entrant :	La règle s'applique seulement pour le trafic entrant.
Les deux :	La règle s'applique dans les deux directions.

• Adresse source - spécifiez l'adresse source.

Pour spécifier l'adresse source, sélectionnez le type d'adresse dans le menu et indiquez les éléments demandés. Les options suivantes sont disponibles :

Toutes :	La règle s'applique à toutes les adresses sources.
Hôte :	La règle ne s'applique que si la source est un hôte spécifique. Vous devez saisir l'adresse IP de l'hôte.
Réseau :	La règle ne s'applique que si la source est un réseau spécifique. Vous devez saisir l'adresse IP et le masque du réseau.
Hôte local :	La règle ne s'applique que si la source est l'hôte local. Si vous utilisez plusieurs interfaces réseau, sélectionnez dans le menu l'interface réseau à laquelle la règle s'applique. Si vous souhaitez que la règle s'applique à tous les hôtes locaux, sélectionnez **Tous**.
Réseau local :	La règle ne s'applique que si la source est le réseau local. Si vous êtes connecté à plusieurs réseaux, sélectionnez dans le menu le réseau auquel la règle s'applique.Si vous souhaitez que la règle s'applique à tous les réseaux locaux, sélectionnez **Tous**.

Adresse source - saisissez l'adresse IP, le masque ou cochez Local si la règle s'applique à l'ordinateur local. Si vous avez sélectionné TCP ou UDP comme protocole vous pouvez définir un port spécifique ou une plage entre 0 et 65535. Si vous voulez que la règle s'applique à tous les ports, sélectionnez **Tous**.

• Adresse de destination - spécifiez l'adresse de destination.

Pour spécifier l'adresse de destination, sélectionnez le type d'adresse dans le menu et indiquez les éléments demandés. Les options suivantes sont disponibles :

Toutes :	La règle s'applique à toutes les adresses de destination.
Hôte :	La règle ne s'applique que si la destination est un hôte spécifique. Vous devez saisir l'adresse IP de l'hôte.
Réseau :	La règle ne s'applique que si la destination est un réseau spécifique. Vous devez saisir l'adresse IP et le masque du réseau.
Hôte local :	La règle ne s'applique que si la destination est l'hôte local. Si vous utilisez plusieurs interfaces réseau, sélectionnez dans le menu l'interface réseau à laquelle la règle s'applique. Si vous souhaitez que la règle s'applique à tous les hôtes locaux, sélectionnez **Tous**.
Réseau local :	La règle ne s'applique que si la destination est le réseau local. Si vous êtes connecté à plusieurs réseaux, sélectionnez dans le menu le réseau Réseau local auquel la règle s'applique. Si vous souhaitez que la règle s'applique à tous les réseaux locaux, sélectionnez **Tous**.

Adresse source - saisissez l'adresse IP, le masque ou cochez Local si la règle s'applique à l'ordinateur local. Si vous avez sélectionné TCP ou UDP comme protocole vous pouvez définir un port spécifique ou une plage entre 0 et 65535. Si vous voulez que la règle s'applique à tous les ports, sélectionnez **Tous**.

• Événements réseau - si vous avez sélectionné TCP ou UDP comme protocole, sélectionnez l'événement réseau auquel la règle s'applique.
Cliquez sur **OK** pour fermer la fenêtre des paramètres avancés.

Cliquez sur **Ajouter** pour ajouter la règle de pare-feu.

8.3.3. Gestion des règles

Les règles créées jusque-là pour le profil en cours sont affichées dans le tableau.

Cochez la case **Processus système cachés** pour cacher les règles concernant les processus systèmes ou les processus BitDefender.

Les règles sont listées dans l'ordre de leur priorité, commençant par le haut, c'est à dire que la première règle a la plus haute priorité. Cliquez sur Editer un profil pour entrer dans l'affichage Vue Détaillée afin de changer leur priorité en les déplaçant de haut en bas.

Pour effacer une règle, sélectionnez-la et cliquez sur le bouton **Effacer règle**.

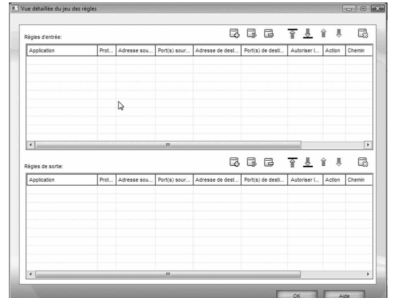
Pour modifier une règle, sélectionnez-la et cliquez sur le bouton **Éditer règle** ou double-cliquez la règle.



Note
Un menu contextuel est également disponible. Il contient les options suivantes : Supprimer, Editer et Ajouter.

8.3.4. Modifier les profils

Vous pouvez modifier un profil en cliquant sur **Editer le profil**. La fenêtre suivante apparaîtra :



Paramètres détaillés

Les règles sont divisées en 2 catégories : règles entrantes et règles sortantes. Vous pouvez voir l'utilisation et les paramètres de chaque règle (adresse source, adresse de destination, ports source, ports de destination, action, etc.)
Pour supprimer une règle, il suffit de la sélectionner et de cliquer sur le bouton **Effacer la règle.**

Pour supprimer toutes les règles, cliquez sur le bouton **Nettoyer liste.** Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton **Éditer la règle** ou double-cliquez dessus. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

Vous avez la possibilité d'augmenter ou de diminuer la priorité d'une règle. Cliquez sur le bouton **Augmenter** pour augmenter d'un niveau la priorité de la règle sélectionnée, ou cliquez sur le bouton **Diminuer** pour diminuer d'un niveau la priorité de la règle sélectionnée. Pour attribuer la priorité la plus élevée à une règle, cliquez sur le bouton **Déplacer en premier.** Pour attribuer la priorité la plus faible à une règle, cliquez sur le bouton **Déplacer en dernier**.

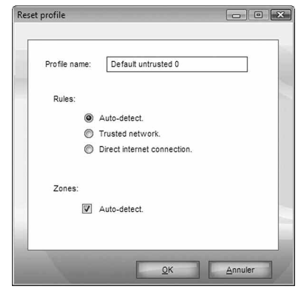


Note
Un menu contextuel est également disponible. Il contient les options suivantes : Ajouter une règle, Éditer la règle, Effacer la règle, Monter, Descendre, Déplacer en premier, Déplacer en dernier et Nettoyer liste.

Cliquez sur **OK** pour fermer la fenêtre.

8.3.5. Réinitialisation des profils

Les utilisateurs avancés ont la possibilité de reconfigurer le profil du pare-feu afin d'optimiser sa protection ou de le personnaliser en fonction de leurs besoins. Pour réinitialiser le profil du pare-feu, cliquez sur Réinitialiser le profil. La fenêtre suivante apparaît :



Réinitialiser le profil

Vous pouvez configurer les options suivantes :

- **Nom du profil** - saisissez un nouveau nom dans la zone de texte.
- **Règles** - spécifiez le type de règles à créer pour les applications du système.

Les options suivantes sont disponibles :

Détection automatique :	Permet à BitDefender de détecter la configuration réseau et de créer un ensemble de règles élémentaires appropriées.
Réseau fiable :	Crée un ensemble de règles élémentaires appropriées à un réseau fiable.
Connexion Internet directe :	Crée un ensemble de règles élémentaires appropriées à une connexion directe à Internet.

- **Zones** - vérifie la Détection automatique pour permettre à BitDefender de créer des zones appropriées pour les réseaux détectés.

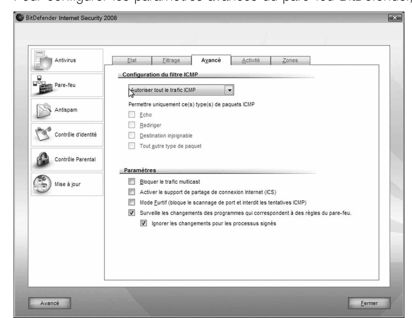
Cliquez sur OK pour fermer la fenêtre et réinitialiser le profil.



Important
Si vous choisissez de reconfigurer le profil du pare-feu, toutes les règles que vous avez ajoutées dans cette section seront perdues.

8.4. Paramètres avancés

Pour configurer les paramètres avancés du pare-feu BitDefender, cliquez sur **Pare-feu > Avancé** dans la console des paramètres. La fenêtre suivante apparaît :



Paramètres avancés

Dans cette rubrique vous pouvez configurer les paramètres avancés du Pare-feu BitDefender. Les paramètres avancés vous permettent de spécifier les règles pour le trafic ICMP (Paramètres du trafic ICMP) et de bloquer le trafic multicast, de partager votre connexion Internet ou de rendre votre ordinateur invisible pour les codes malicieux ou les hackers (Propriétés).

8.4.1. Configuration des paramètres de filtrage ICMP

Depuis le menu, vous pouvez choisir l'une des politiques suivantes pour filtrer le trafic ICMP :

- **Autoriser tout le trafic ICMP** - autorise tout le trafic ICMP.
- **Bloquer tout le trafic ICMP** - bloque tout le trafic ICMP.
- **Personnaliser le filtrage ICMP** - personnalise la façon dont le ICMP trafic est filtré. Vous avez la possibilité de sélectionner le type de paquets ICMP à autoriser.

Les options suivantes sont disponibles :

Echo : Cette option active les messages de Réponses d'Echo et de Demandes d'Echo. La Demande d'Echo est un message ICMP qui envoie un paquet de données à l'hôte et attend que cette donnée revienne dans une Réponse Echo. L'hôte doit répondre à toutes les Demandes d'Echo avec une Réponse d'Echo qui contient les données exactes reçues dans le message de demande. La Réponse d'Echo est un message ICMP généré en réponse à un message de Demande d'Echo, et est obligatoire pour tous les hôtes et routeurs.

Faire Suivre : C'est un message ICMP qui informe un hôte de faire suivre son information de cheminement (pour envoyer les paquets sur un itinéraire alternatif). Si l'hôte essaie d'envoyer des données à travers un routeur (R1) et un autre routeur (R2) pour atteindre l'hôte, alors qu'un chemin direct depuis l'hôte vers R2 est disponible, la redirection informera l'hôte de ce chemin. Le routeur enverra encore le datagramme original à sa destination. Cependant, si le datagramme contient des informations de routage, ce message ne sera pas envoyé même si un meilleur chemin est disponible.

Destination inaccessible : Il s'agit d'un message ICMP généré par le routeur pour informer le client que le destinataire n'est pas accessible, bien que le datagramme ait une adresse multicast. Les raisons de ce message peuvent inclure la connexion physique à l'hôte qui n'existe pas (la distance est infinie), le protocole ou port indiqué n'est pas actif, ou les données doivent être fragmentées alors que l'option 'ne pas fragmenter' est activée.

Tout autre type de paquets : Avec cette option activée, tout autre package que Echo, Destination inaccessible ou Faire Suivre passera.

- Applique les règles courantes pour le trafic ICMP - applique les règles définies dans la section Etat du module Pare-feu.

8.4.2. Configuration des paramètres avancés du pare-feu

Les paramètres suivants du Pare-feu avancé sont disponibles :

- Bloquer tout le trafic multicast - dépose tous les paquets multicast reçus.

Le trafic multicast est un type de trafic s'adressant à un groupe particulier au sein d'un réseau. Les paquets sont envoyés à une adresse spécifique depuis laquelle les clients multicast peuvent les recevoir si ils le souhaitent. Par exemple, un membre d'un réseau qui dispose d'un tuner TV peut diffuser le flux vidéo en mode broadcast (en l'envoyant à chaque membre du réseau) ou en mode multicast (en envoyant le flux vidéo à une adresse spécifique). Les ordinateurs qui gèrent le multicast peuvent choisir de l'accepter ou le refuser pour le regarder ou non.
Un trafic multicast trop important peut consommer des ressources et de la bande passante de manière excessive. En validant cette option tous les packages multicast seront rejetés. Cependant il n'est pas recommandé d'activer cette option.

- Autoriser le partage de Connexion Internet (ICS) - active le support du partage de connexion Internet en mode ICS.



Note
Cette option active uniquement le support de ce mode de partage qui doit par ailleurs être activé dans votre système d'exploitation.

Le mode ICS (Internet Connection Sharing) permet aux membres d'un réseau local de se connecter à Internet à travers votre ordinateur. Cette fonction est particulièrement appréciable quand vous bénéficiez d'un type de connexion spécial (Ex : connexion sans fil) et que vous voulez la partager avec d'autres membres de votre réseau.
Le fait de partager votre connexion Internet avec les membres d'un réseau local implique une consommation plus importante de ressources et peut comporter certains risques. Cela utilise également un certain nombre de vos ports (ceux ouverts par les membres du réseau qui utilisent votre connexion Internet).

- **Mode camouflé** - il rend votre ordinateur invisible pour les codes malicieux et les hackers. Une façon simple de déterminer si votre ordinateur est vulnérable est de se connecter à ses ports pour voir si ils répondent, cela s'appelle un "Scan de port".

Les individus ou logiciels malicieux n'ont pas besoin de savoir que votre ordinateur existe. L'option Mode camouflé empêchera votre machine de répondre aux tentatives de "scan" visant à trouver quels ports sont ouverts.

- **Détecter les modifications de processus** - contrôle toutes les applications tentant de se connecter à Internet pour savoir si elles ont été modifiées depuis l'ajout de la règle contrôlant leur accès. Si une application a été modifiée, un message d'alerte vous demandera d'autoriser ou de bloquer son accès à Internet.

Les applications sont généralement modifiées par les mises à jour. Il existe toutefois un risque qu'elles soient modifiées par des applications malveillantes ayant pour objectif d'infecter votre ordinateur ainsi que d'autres ordinateurs du réseau.

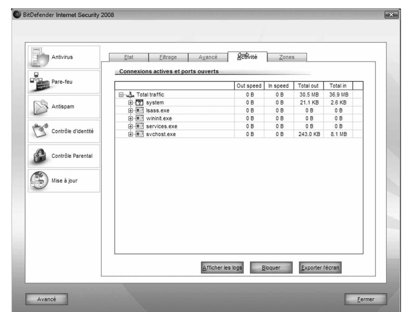


Note
Nous vous recommandons de maintenir cette option activée et de n'autoriser l'accès qu'aux applications ayant été modifiées après la création de la règle contrôlant leur accès.

Les applications signées sont en principe fiables et présentent un niveau de sécurité plus élevé. Cochez la case Ignorer les modifications de **processus pour les applications signées** pour autoriser les applications signées modifiées à se connecter à Internet sans recevoir de message d'alerte sur cet événement.

8.5. Contrôle des connexions

Pour contrôler l'activité en cours du réseau/Internet (via TCP et UDP) répertoriée par application et pour ouvrir le journal du pare-feu BitDefender, cliquez sur **Pare-feu > Activité** dans la console des paramètres. La fenêtre suivante apparaît :



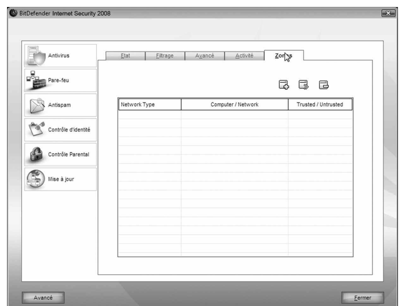
Contrôle des connexions

Le trafic total répertorié par application s'affiche. Chaque application comporte des informations sur les connexions et les ports ouverts, des statistiques sur la vitesse du trafic entrant et sortant et le nombre total de données envoyées/reçues.
La fenêtre indique l'activité du réseau/Internet en temps réel. Lorsque des connexions ou des ports sont fermés, les statistiques correspondantes sont estompées et finissent par disparaître. Il en va de même pour toutes les statistiques correspondant à une application que vous fermez qui génère du trafic ou comporte des ports ouverts.
Cliquez sur **Bloquer** pour créer des règles qui limitent le trafic par les applications, ports ou connexions sélectionnés. Une confirmation vous sera demandée. Vous pouvez accéder aux règles dans la rubrique Trafic pour des paramétrages plus avancés.
Cliquez sur **Exporter l'écran** pour exporter la liste dans un fichier .txt.

Pour obtenir une liste étendue des événements concernant l'utilisation du module Pare-feu (activer/désactiver le Pare-feu, bloquer le trafic, activer le mode camouflé, modifier les paramètres, appliquer un profil) ou des événements générés par les activités détectées par le Pare-feu (analyse des ports, bloquer les tentatives de connexions ou le trafic selon les règles paramétrées), cochez le fichier de rapport du Pare-feu BitDefender que vous trouverez en cliquant sur **Afficher le rapport.** Le fichier se trouve dans le dossier Fichiers Communs de l'utilisateur actuel de Windows, sous le chemin : ...BitDefender\BitDefender Firewall\bdfirewall.txt.

8.6. Zones réseau

Une zone est une adresse IP (ou un ensemble d'adresses IP) pour laquelle une règle spéciale est créée dans un profil. Cette règle peut soit autoriser un accès illimité à votre ordinateur aux utilisateurs du réseau (zone fiable), soit au contraire isoler complètement votre ordinateur des ordinateurs du réseau (zone non fiable). Par défaut, BitDefender détecte automatiquement le réseau auquel vous êtes connecté et ajoute une zone en fonction de la configuration réseau.





Note
Si vous êtes connecté à plusieurs réseaux, plusieurs zones peuvent être ajoutées selon leur configuration.

Des zones fiables sont ajoutées par défaut pour les configurations réseau suivantes :

- **IP privée sans passerelle** - L'ordinateur fait partie d'un réseau local (LAN) et n'est pas connecté à Internet.
- **IP privée avec contrôleur de domaine détecté** - L'ordinateur fait partie d'un réseau LAN et est connecté à un domaine

Des zones non fiables sont ajoutées par défaut pour les configurations réseau suivantes :

- **Sans fil ouvert (non sécurisé)** - L'ordinateur fait partie d'un réseau local sans fil (WLAN).

Pour configurer les zones réseau, cliquez sur **Pare-feu > Zones** dans la console des paramètres. La fenêtre suivante apparaît :

Les zones réseau correspondant au profil en cours sont affichées dans le tableau. Chaque zone permet d'accéder aux informations suivantes : le type de réseau (réseau Ethernet, sans fil, PPP, etc.), l'ordinateur ou le réseau associé à la zone et si la zone est fiable ou non.

Pour modifier une zone, sélectionnez-la, puis cliquez sur le bouton **Modifier la zone** ou double-cliquez dessus.

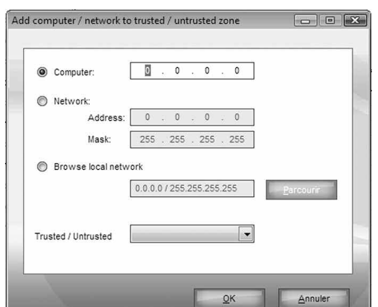
Note
Par défaut, BitDefender ajoute les réseaux sans fil ouverts en tant que zones non fiables. Si vous êtes connecté à un réseau sans fil ouvert ad hoc avec des ordinateurs fiables (à la maison ou entre amis), il peut être utile de modifier la zone associée. Pour pouvoir partager des ressources avec les autres utilisateurs du réseau, vous devez configurer le réseau en tant que zone fiable.

Pour supprimer une zone, sélectionnez-la et cliquez sur le bouton **Supprimer la zone.**

8.6.1. Ajout de zones

Vous pouvez ajouter des zones manuellement. Cela peut vous permettre, par exemple, de partager des fichiers dans un réseau sans fil ouvert uniquement avec vos amis (en ajoutant leurs ordinateurs en tant que zones fiables) ou de bloquer l'ordinateur d'un réseau fiable (en l'ajoutant en tant que zone non fiable).

Pour ajouter une nouvelle zone, cliquez sur le bouton **Ajouter une zone.** La fenêtre suivante apparaît :



Ajouter une zone

Pour ajouter une zone, procédez comme suit :

1. Sélectionnez un **ordinateur** d'un réseau local ou un réseau local entier que vous souhaitez ajouter en tant que zone. Vous pouvez utiliser l'une des méthodes suivantes :

- Pour ajouter un ordinateur spécifique, sélectionnez Ordinateur et indiquez son adresse IP.
- Pour ajouter un réseau spécifique, sélectionnez **Réseau** et indiquez son adresse IP et son masque.
- Parcourez les réseaux locaux pour rechercher et ajouter un ordinateur ou un réseau.

Pour parcourir les réseaux locaux, sélectionnez Parcourir le réseau local, puis cliquez sur Parcourir. Une nouvelle fenêtre apparaît affichant tous les réseaux auxquels vous êtes connecté ainsi que tous les membres de chaque réseau.

Sélectionnez dans la liste l'ordinateur ou le réseau que vous souhaitez ajouter en tant que zone, puis cliquez sur **OK**.

2. Sélectionnez dans le menu le type de zone que vous souhaitez créer (fiable ou non fiable).

3. Cliquez sur **OK** pour ajouter la zone.

9. Antispam

BitDefender Antispam utilise des innovations technologiques de pointe et des filtres antispam répondant aux normes industrielles qui permettent d'éliminer les spams avant qu'ils n'atteignent la boîte aux lettres de l'utilisateur.

La partie **Antispam** de ce Manuel d'utilisation contient les thèmes suivants :

- Aperçu de l'antispam
- Etat Antispam
- Paramètres Antispam
- Intégration dans les clients de messagerie

9.1. Aperçu de l'antispam

Le Spam est un problème croissant, à la fois pour les particuliers et les entreprises. Vous ne voudriez pas que vos enfants tombent sur certains emails, vous pourriez perdre votre travail (pour une perte de temps trop grande ou parce que vous recevez trop de messages à caractère pornographique sur votre email professionnel) et vous ne pouvez pas empêchez les gens d'en envoyer. L'idéal serait de pouvoir arrêter de les recevoir. Malheureusement, le SPAM arrive dans un large éventail de formes et de tailles, et il en existe beaucoup.

9.1.1. Filtres antispam

Le moteur Antispam de BitDefender utilisent sept filtres différents qui protègent votre boîte aux lettres des SPAM : List Blanche, Liste Noire, Filtre jeu de caractères, Filtre Image, Filtre URL, Filtre Heuristique et Filtre Bayesien.


Note
Vous pouvez activer/désactiver chacun de ces filtres dans le module Antispam, rubrique Paramètres.

Liste Blanche / Liste Noire

La majorité des utilisateurs communiquent régulièrement avec un groupe de personnes ou reçoivent des messages de la part des entreprises et compagnies du même domaine. En utilisant les **listes amis/spammeurs,** vous pouvez déterminer aisément de quelles personnes vous voulez recevoir des messages et de quelles personnes vous ne voulez plus en recevoir.


Note
Liste Blanche / Liste Noire sont aussi connues en tant que Liste des Amis/ Liste des Spammeurs.

Les **listes des amis/spammeurs** peuvent être gérées depuis la Console des paramètres ou la Barre d'outils Antispam intégrée aux clients de messagerie les plus utilisés.


Note
Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses email à la Liste des Amis. BitDefender ne bloque pas les messages provenant de cette liste ; ajouter des amis vous aide à laisser passer les messages légitimes.

Filtre de caractères

De nombreux spams sont écrits en caractères cyrilliques et/ou asiatiques. Le filtre de caractères détecte ce type de messages et les enregistre en tant que SPAM.

Filtre d'Image

Eviter le filtre heuristique est devenu un tel challenge que la boîte de réception se remplit de plus en plus avec des messages ne contenant qu'une image avec du contenu non sollicité. Pour faire face à ce problème, BitDefender intègre le Filtre Image qui compare la signature image de l'e-mail avec celle de la base de données de BitDefender. Si la signature correspond, l'email sera marqué comme SPAM. Sa nouvelle technologie S.I.D. (Spam Image Distance) permet également de détecter des images "proches" de celles connues dans sa base par comparaison de la structure de l'image (nombre de pixels de chaque couleur, etc.).

Filtre URL

La plupart des spams comportent des liens vers des destinations Web. Ces destinations sont souvent des pages à caractères publicitaires offrant la possibilité de faire des achats et sont parfois utilisées pour le phishing.
BitDefender maintient une base de données de ce type de liens. Le filtre URL compare tous les liens URL d'un message à sa base de données. Si un lien correspond, le message est enregistré en tant que SPAM.

Filtre heuristique

Le Filtre Heuristique effectue des tests sur tous les composants du message (pas seulement l'en-tête mais aussi le corps du message en html ou format texte), cherchant des mots spécifiques, phrases, liens ou autres caractéristiques du spam. En fonction des résultats de l'analyse, un score de SPAM est ajouté au message. Le filtre détecte aussi les messages marqués comme SEXUELLEMENT EXPLICITES dans leur objet et les enregistre en tant que SPAM.


Note
Depuis le 19 mai 2004, le spam avec un contenu sexuel doit inclure l'avertissement SEXUELLEMENT EXPLICITE dans l'objet, contre risque d'amendes pour violation de la loi.

Filtre Bayesien

Le module **Filtre Bayesien** classe les messages grâce à des informations statistiques sur les occurrences de certains mots dans les messages classifiés comme SPAM comparés avec ceux qui sont déclarés NON-SPAM (par vous-même ou par le filtre heuristique).
Ceci signifie que, par exemple, si un certain mot de 4 lettres apparaît plus fréquemment dans les spam, il est normal de supposer que la probabilité que le prochain message le contenant soit aussi un SPAM soit forte. Tous les mots pertinents d'un message sont pris en considération. En synthétisant les informations statistiques, la probabilité globale qu'un message soit un SPAM est calculée. Ce module présente une autre caractéristique intéressante : il peut être entraîné. Il s'adapte rapidement
au type de messages reçus par l'utilisateur, et enregistre des informations concernant ces messages.
Pour fonctionner d'une manière efficace, le filtre doit être entraîné en lui présentant des échantillons de SPAM et de messages corrects. Parfois le filtre doit également être corrigé ou invité à changer d'avis quand il a pris la mauvaise décision.



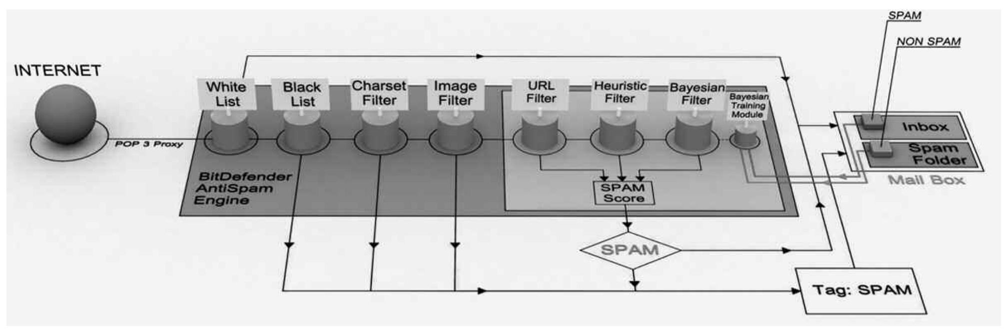
Important
Vous pouvez corriger le module Bayesien utilisant les boutons Spam et Non Spam de la barre d'outils Antispam.



Note
Chaque fois que vous effectuez une mise à jour :
• Des nouvelles signatures d'images seront ajoutées au Filtre Image.
• Des nouveaux liens seront ajoutés au Filtre URL.
• Des nouvelles règles seront ajoutées au Filtre NeuNet (Heuristique).
Cette manipulation aide à renforcer l'efficacité du moteur Antispam.
Pour vous protéger des Spammeurs, BitDefender peut effectuer des mises à jour automatiques. Maintenez l'option Mise à jour automatique activée.

9.1.2. Fonctionnement de l'antispam

Le schéma ci-dessous vous montre comment fonctionne BitDefender.



Fonctionnement de l'antispam

Les filtres antispam du schéma ci-dessus (Liste Blanche, Liste Noire, Filtre jeu de caractères, Filtre Image, Filtre URL, Filtre Heuristique et Filtre Bayesien) sont utilisés en série par BitDefender, pour déterminer si tel ou tel email est autorisé à arriver dans votre boîte aux lettres ou non.
Chaque e-mail qui provient d'Internet est d'abord vérifié avec la Liste Blanche/Liste Noire. Si l'adresse de l'envoyeur est trouvée dans la Liste Blanche, l'email est directement déplacé dans votre **Boîte de réception.**
Sinon le filtre Liste Noire récupérera l'adresse de l'envoyeur et vérifiera si elle figure dans sa liste.
L'email sera marqué comme SPAM et déplacé dans le dossier **Spam** (localisé dans Microsoft Outlook) si l'adresse est dans la liste. Autrement, le Jeu de caractères vérifiera si l'email est écrit en caractères cyrilliques ou asiatiques. Si tel est le cas, le message sera marqué comme Spam et déplacé vers le dossier Spam.
Si l'email n'est pas écrit en caractères asiatiques ou cyrilliques, il sera transféré au Filtre Image. Le Filtre Image détectera tous les messages contenant des images attachées contenant du contenu prohibé.

Le Filtre URL recherchera des liens et les comparera à la base de données de BitDefender. Si le lien correspond, il sera marqué comme SPAM.

Le Filtre Heuristique effectuera une série de tests sur les composants du message, cherchant des mots, des phrases, des liens ou d'autres caractéristiques propres au SPAM. L'email se verra ainsi attribué une note Spam.



Note
Si l'email a un objet SEXUELLEMENT EXPLICITE, BitDefender le considérera comme du SPAM.

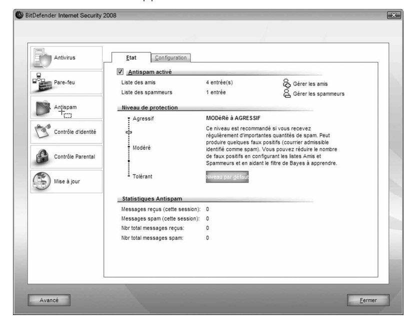
Le module Filtre Bayesien analysera plus en profondeur le message grâce à des informations statistiques s'appuyant sur des taux d'apparition de mots spécifiques dans des messages considérés comme SPAM comparé à ceux considérés comme NON-SPAM (par vous ou par le filtre Heuristique). Il ajoutera également un score de spam au message. Le message sera marqué comme Spam si la somme des scores (score URL + score heuristique + score Bayesien) dépasse le seuil de spam d'un message (défini par l'utilisateur dans la rubrique Antispam comme niveau de tolérance).



Important
Si vous utilisez un autre client mail que Microsoft Outlook ou Microsoft Outlook Express, il est conseillé de créer une règle pour déplacer les messages marqués SPAM par BitDefender dans un dossier de quarantaine personnalisé. BitDefender appose le préfixe [SPAM] aux sujets des messages considérés comme SPAM.

9.2. Etat de l'Antispam

Pour configurer la protection antispam, cliquez sur **Antispam > État** dans la console des paramètres.
La fenêtre suivante apparaît :



Etat de l'Antispam

Dans cette section vous pouvez configurer le module Antispam et voir des informations sur son activité.



Important
Pour vous éviter de recevoir du spam, gardez votre filtre Antispam activé.
Dans la rubrique Statistiques vous pouvez consulter les statistiques concernant le module Antispam. Ces résultats sont présentés par sessions (depuis que vous avez démarré votre ordinateur). Vous pouvez aussi consulter un sommaire de l'activité antispam (depuis l'installation du filtre Antispam).

Pour configurer le module Antispam, il est nécessaire de suivre les étapes suivantes :

9.2.1. Etape 1 sur 2 - Définir le niveau de tolérance

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié. Il ya 5 niveaux de tolérance :

Tâche d'analyse par défaut	Description
Tolérant	Offre une protection pour les comptes qui reçoivent beaucoup d'emails commerciaux légitimes. Le filtre laissera passer la plupart des emails, mais produira un certain nombre de "faux négatifs" (Spam classés comme des mails légitimes).
Tolérant à Modéré	Offre une protection pour les comptes qui reçoivent quelques emails commerciaux. Le filtre laissera passer la plupart des emails, mais produira un certain nombre de "faux négatifs" (Spam classés comme des mails légitimes).
Modéré	Offre une protection pour les comptes de messagerie standard. Le filtre bloquera la plupart des spams, tout en évitant les faux positifs.
Modéré à agressif	Offre une protection pour les messageries qui reçoivent régulièrement un gros volume de spam. Le filtre ne laissera quasiment pas passer de spam mais peut éventuellement produire des faux positifs (emails légitimes considérés comme Spam).
Agressif	Offre une protection pour les messageries qui reçoivent régulièrement un très grand nombre de spam. Le filtre ne laissera quasiment pas passer de spam mais peut éventuellement produire des faux positifs (emails légitimes considérés comme Spam).

Configurez la liste d'amis / de spammeurs et entraînez le moteur d'apprentissage bayésien dans le but de réduire le nombre de faux positifs.
Ajouter vos contacts à la liste d'amis dans le but de réduire le nombre de faux positifs.
Pour définir le niveau de protection par défaut (de Modéré à Agressif), cliquez sur Niveau par défaut.

9.2.2. Etape 2 sur 2 - Remplir la liste d'adresses

La liste d'adresses contient des informations sur les adresses e-mail vous envoyant des messages légitimes ou du spam.

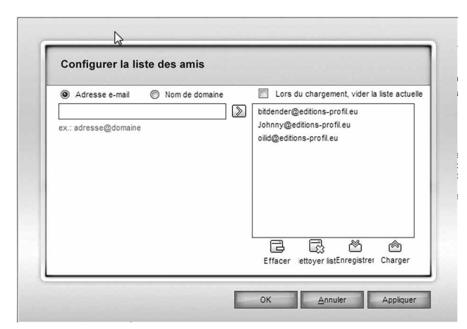
Liste des amis

La **liste d'amis** est une liste de toutes les adresses email dont vous accepterez les messages, quel que soit leur contenu. Les messages de vos amis ne seront jamais considérés comme spam, même si leur contenu ressemble au spam.



Note
Tous les messages provenant d'une adresse contenue dans la liste d'amis seront automatiquement déposés dans votre boîte de réception d'email.

Pour gérer la **Liste d'amis** cliquez sur >>> (correspondant à la **Liste des amis**) ou sur le **bouton Amis** de la barre d'outils Antispam.



Liste des amis

Ici vous pouvez ajouter ou effacer des amis dans la liste.
Si vous désirez ajouter une adresse email cliquez dans le champ Adresse Email, introduisez-la et cliquez sur la flèche. L'adresse apparaîtra dans la liste d'amis.



Important
Syntaxe : name@domain.com

Si vous désirez rajouter un domaine cliquez sur le champ Nom domaine, entrez le nom de domaine puis cliquez sur. Le domaine apparaît dans la liste d'amis.



Important
Syntaxe :
• <@domain.com>, <*domain.com> et <domain.com> - tous les messages en provenance de <domain.com> seront dirigés vers votre **Boîte de réception** quel que soit leur contenu ;
• <*domain*> - tous les messages provenant de <domain> (quel que soit le suffixe) seront dirigés vers votre Boîte de réception quel que soit leur contenu ;
• <*com> - tous les messages ayant comme suffixe du domaine <com> seront redirigés vers votre **Boîte de réception** quel que soit leur contenu ;
Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le bouton Syntaxe :
Effacer. Si vous cliquez sur le bouton **Vider la liste** vous supprimerez toutes les entrées de la liste, mais attention : il sera alors impossible de les récupérer.
Utilisez les boutons Sauvegarder/ Charger pour sauvegarder/charger la Liste des amis vers un emplacement désiré. Le fichier a l'extension .bwl.
Pour supprimer le contenu de la liste en cours d'utilisation quand vous chargez une liste sauvegardée auparavant, choisissez Au chargement, **nettoyer la liste en cours.**



Note
Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses email à la Liste des Amis. BitDefender ne bloque pas les messages provenant de cette liste ; ajouter des amis vous aide à laisser passer les messages légitimes.

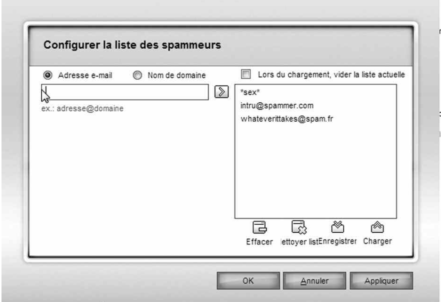
Cliquez sur Appliquer et **OK** pour sauvegarder et fermer la **liste d'amis**.

Liste des Spammeurs

La liste des spammeurs est une liste de toutes les adresses e-mail dont vous ne voulez recevoir aucun message, quel que soit son contenu.



Note
Tout message en provenance d'une adresse de la liste des spammeurs sera automatiquement marqué SPAM sans autre traitement.
Pour gérer la la liste des Spammeurs cliquez sur (correspondant à la liste des Spammeurs) ou sur le bouton Spammeurs de la barre d'outils Antispam.



Liste des Spammeurs

Ici vous pouvez ajouter ou effacer des spammeurs dans la liste.
Si vous désirez ajouter une adresse email cochez l'option Adresse Email, entrez la et cliquez sur la flèche.
L'adresse apparaîtra dans la liste des Spammeurs.



Important
Syntaxe : <name@domain.com>.
Si vous désirez rajouter un domaine cochez l'option Nom de domaine, entrez le et puis cliquez sur la flèche. Le domaine apparaîtra dans la liste des Spammeurs.



Important
Syntaxe :
• <@domain.com>, <*domain.com> et <domain.com> - tous les messages provenant de <domain.com> seront étiquetés comme SPAM ;
• <*domain*> - tous les messages de <domain> (quel que soit le suffixe) seront étiquetés comme SPAM ;
• <*com> - tous les messages provenant d'un domaine avec un suffixe <com> seront étiquetés comme SPAM.

Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**. Si vous cliquez sur le bouton **Vider la liste** vous supprimerez toutes les entrées de la liste, mais attention : il sera alors impossible de les récupérer.
Utilisez les boutons **Sauvegarder/** **Charger** pour sauvegarder/charger la **liste des Spammeurs** vers un emplacement désiré. Le fichier a l'extension .bwl. Pour supprimer le contenu de la liste en cours d'utilisation quand vous chargez une liste sauvegardée auparavant, choisissez Au chargement, nettoyer la liste en cours.

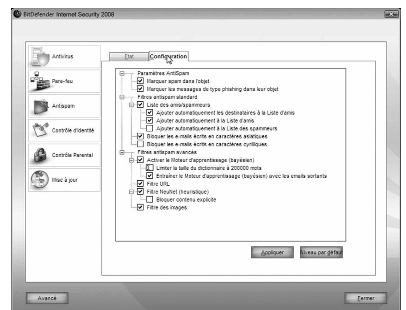


Cliquez sur Appliquer et **OK** pour sauvegarder et fermer la liste des spammeurs.



Important
Si vous désirez réinstaller BitDefender, nous vous conseillons de sauvegarder la liste Amis / Spammeurs avant, et de la charger après l'installation.

9.3. Configuration de l'Antispam



Pour configurer les paramètres antispam, cliquez sur **Antispam > Paramètres** dans la console des paramètres. La fenêtre suivante apparaît :

Configuration de l'Antispam

Ici vous pouvez activer/désactiver chacun des filtres Antispam et spécifier certains des paramétrages concernant le module Antispam. Trois catégories d'options sont disponibles (Paramètres Antispam, Filtres Antispam standard et Filtres Antispam avancés), organisées dans un menu déroulant, similaire aux menus Windows.



Note
Cliquez sur une case "+" pour ouvrir une arborescence et sur une case "-" pour la fermer.

9.3.1. Configuration de l'Antispam

- **Marquer spam dans l'objet** - tous les messages étant considérés comme spam recevront un préfixe [spam] dans leur objet.
- **Marquer les messages de type phishing dans leur objet** - tous les messages étant considérés comme phishing recevront un préfixe [phishing] dans leur objet.

9.3.2. Filtres antispam de base

- **Listes amis / Spammeurs** - active/désactive les listes amis / spammeurs ;
- **Ajouter automatiquement à la liste d'amis** - pour ajouter les expéditeurs à la liste d'amis.
- **Ajouter automatiquement à la Liste d'amis** - la prochaine fois que vous cliquerez sur le bouton **Pas Spam** de la barre d'outils Antispam, l'expéditeur sera automatiquement ajouté à la Liste d'amis.
- **Ajouter automatiquement à la Liste des spammeurs** - la prochaine fois que vous cliquerez sur le bouton **Spam** de la barre d'outils Antispam, l'expéditeur sera automatiquement ajouté à la Liste des spammeurs.



Note
Les boutons **Pas Spam** et **Spam** sont utilisés pour former le filtre Bayesien.

- **Bloquer les caractères asiatiques** - bloque les messages écrits en caractères asiatiques.
- **Bloquer les caractères cyrilliques** - bloque les messages écrits en caractères cyrilliques.

9.3.3. Filtres antispam avancés

- **Active le moteur d'apprentissage** - active/désactive le moteur d'apprentissage (bayesien).
- **Limiter la taille du dictionnaire à 200.000 mots** - vous pouvez limiter la taille du dictionnaire bayesien – Plus la taille est réduite, plus c'est rapide. Plus la taille est importante, plus c'est précis.



Note
La taille recommandée est de 200.000 mots.

- **Entraîner le moteur d'apprentissage (bayesien) sur les emails sortants** - entraîne le moteur d'apprentissage (bayesien) sur les emails sortants.
- **Filtre URL** - active/désactive le Filtre URL ;
- **Filtre heuristique** - active/désactive le Filtre heuristique ;
- **Bloquer le contenu explicite** - active/désactive la détection de messages contenant des objets SEXUELLEMENT EXPLICITE ;
- **Filtre des images** - active/désactive le Filtre des images.



Note
Pour activer/désactiver une option cochez/décochez la case correspondante.

Cliquez sur **Appliquer** pour sauvegarder les modifications ou cliquez sur **par Défaut** pour charger les paramètres par défaut.

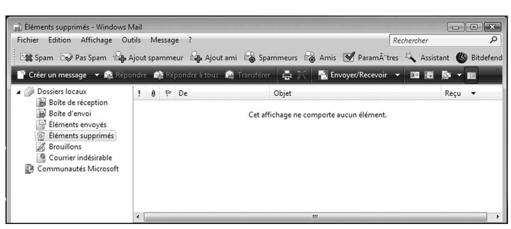
9.4. Intégration dans les clients de messagerie

BitDefender s'intègre directement dans les clients de messagerie suivants au moyen d'une barre d'outils intuitive et conviviale :

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

9.4.1. Barre d'outils Antispam

La barre d'outil Antispam se trouve dans la partie supérieure de votre client de messagerie.



Barre d'outils Antispam



Important
La principale différence entre BitDefender Antispam pour Microsoft Outlook et Outlook Express / Windows Mail est le fait que les messages SPAM sont déplacés dans le dossier Spam de Microsoft Outlook et dans le dossier Effacés pour Outlook Express / Windows Mail. Dans les deux cas les messages reçoivent l'étiquette SPAM rajoutée à leurs objets. Le dossier Spam créé par BitDefender Antispam pour Microsoft Outlook est situé au même niveau que les objets de la liste répertoires (Calendrier, Contacts, etc..).

Chaque bouton de la barre d'outils de BitDefender sera expliqué ci-dessous :

- **Spam** - Cliquez dessus pour envoyer un message au module bayesien indiquant que le message respectif est un spam. Le message recevra l'étiquette SPAM et sera déplacé dans le dossier Spam. Les futurs messages ayant les mêmes caractéristiques seront aussi considérés comme SPAM.



Note
Vous pouvez choisir un ou plusieurs messages.

- **Pas Spam** - Cliquez dessus pour envoyer un message au module bayesien indiquant que le message respectif n'est pas un spam et BitDefender ne devrait pas l'étiqueter. Le message sera déplacé du dossier Spam vers la Boîte de réception. Les futurs messages ayant les mêmes caractéristiques ne seront pas considérés comme SPAM.

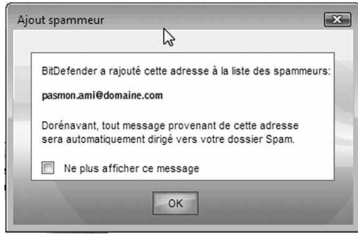


Note
Vous pouvez choisir un ou plusieurs messages.



Important
Le bouton Pas Spam devient actif quand vous choisissez un message marqué spam par BitDefender (ces messages se trouvent d'habitude dans le répertoire Spam).

- **Ajout spammeur** - Cliquez dessus pour ajouter l'expéditeur du message à votre **liste des spammeurs.**



Ajout de spammeur

Choisir Ne plus afficher ce message pour ne plus être consulté lors d'un rajout de spammeur dans la liste.
Cliquez sur **OK** pour fermer la fenêtre. Les futurs messages provenant de cette adresse seront considérés comme SPAM.



Note
Vous pouvez choisir un seul expéditeur ou plusieurs.

- **Ajout ami** - Cliquez dessus pour ajouter l'expéditeur des messages choisis à votre Liste d'amis.



Ajouter un ami

Choisir Ne plus afficher ce message pour ne plus être averti lors d'un rajout de ami dans la liste.
Cliquez sur OK pour fermer la fenêtre. Les futurs messages provenant de cette adresse seront toujours dirigés vers votre boîte de réception quel que soit leur contenu.



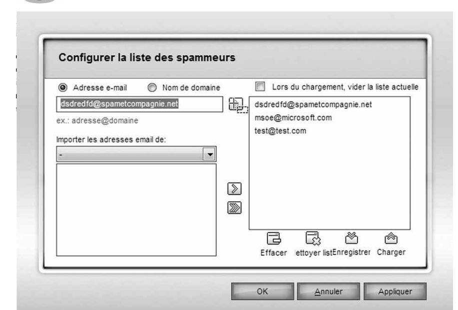
Note
Vous pouvez choisir un seul expéditeur ou plusieurs.

- Spammeurs - Cliquez dessus pour gérer la liste des spammeurs – elle contient toutes les adresses dont vous ne voulez pas recevoir des messages, quel que soit leur contenu.



Note

Tout message en provenance d'une adresse de la liste des spammeurs sera automatiquement marqué SPAM sans autre traitement.



Liste des Spammeurs

Ici vous pouvez ajouter ou effacer des spammeurs dans la liste. Si vous désirez ajouter une adresse email, cliquez dans le champ Adresse e-mail, entrez la et cliquez sur . L'adresse apparaîtra dans la **liste de spammeurs.**



Important

Syntaxe : <name@domain.com>.

Si vous désirez rajouter un domaine cliquez sur le champ Nom domaine, entrez le nom de domaine puis cliquez sur .

Le domaine apparaît dans la liste des spammeurs.



Important

Syntaxe :

- <@domain.com>, <*domain.com> et <domain.com> - tous les messages provenant de <domain.com> seront étiquetés comme SPAM ;
- <*domain*> - tous les messages de <domain> (quel que soit le suffixe) seront étiquetés comme SPAM ;
- <*com> - tous les messages provenant d'un domaine avec un suffixe <com> seront étiquetés comme SPAM.

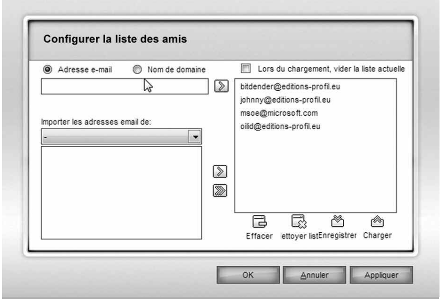
Pour importer une adresse e-mail depuis le Carnet **d'Adresses Windows / Dossiers Outlook Express** et l'envoyer vers Microsoft **Outlook / Outlook Express / Windows Mail,** sélectionnez l'option appropriée depuis le menu déroulant Importer les adresses e-mail depuis.
Pour **Microsoft Outlook Express / Windows Mail,** une nouvelle fenêtre apparaîtra dans laquelle vous pouvez sélectionner le répertoire qui contient les adresses email que vous désirez ajouter dans la **liste des Spammers.** Choisissez-les et cliquez sur Sélectionnez.
Dans les deux cas les adresses email apparaîtront dans la liste des imports. Sélectionnez celles désirées et cliquez pour les **ajouter dans la liste des spammers.** Si vous cliquez sur toutes les adresses email seront ajoutées à la liste. Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**. Si vous cliquez sur le bouton **Vider la liste** vous supprimerez toutes les entrées de la liste, mais attention : il sera alors impossible de les récupérer.
Utilisez les boutons **Sauvegarder/** **Charger** pour sauvegarder/charger la liste des Spammeurs vers un emplacement désiré. Le fichier a l'extension .bwl.
Pour supprimer le contenu de la liste en cours d'utilisation quand vous chargez une liste sauvegardée auparavant, choisissez **Au chargement, nettoyer la liste en cours.**
Cliquez sur **Appliquer** et **OK** pour sauvegarder et fermer la **liste des spammeurs**.

- **Amis -** Cliquez dessus pour gérer la liste des amis, elle contient toutes les adresses dont vous voulez recevoir les messages, quel que soit leur contenu.



Note

Tous les messages provenant d'une adresse contenue dans la **liste d'amis** seront automatiquement déposés dans votre boîte de réception d'email.



Liste des amis

Ici vous pouvez ajouter ou effacer des amis dans la liste. Si vous désirez ajouter une adresse email cliquez dans le champ Adresse e-mail, entrez la et cliquez sur le bouton . L'adresse apparaîtra dans la **liste d'amis.**



Important, Syntaxe :

Si vous désirez rajouter un domaine cliquez sur le champ **Nom domaine,** *entrez le nom de domaine puis cliquez sur name@domain.com. Le domaine apparaît dans la* **liste d'amis.**



Important

Syntaxe :

- <@domain.com>, <*domain.com> et <domain.com> - tous les messages en provenance de <domain.com> seront dirigés vers votre Boîte de réception quel que soit leur contenu ;
- <*domain*> - tous les messages provenant de <domain> (quel que soit le suffixe) seront dirigés vers votre Boîte de réception quel que soit leur contenu ;
- <*com> - tous les messages ayant comme suffixe du domaine <com> seront redirigés vers votre Boîte de réception quel que soit leur contenu ;

Pour importer une adresse e-mail depuis le **Carnet d'Adresses Windows / Dossiers Outlook Express** et l'envoyer vers **Microsoft Outlook / Outlook Express / Windows Mail**, sélectionnez l'option appropriée depuis le menu déroulant **Importer les adresses e-mail** depuis. Pour Microsoft Outlook Express / Windows Mail une nouvelle fenêtre apparaîtra dans laquelle vous pouvez sélectionner le répertoire qui contient les adresses email que vous désirez ajouter dans la liste des Amis. Choisissez-les et cliquez sur **Sélectionnez**.

Dans les deux cas les adresses email apparaîtront dans la liste des imports. Sélectionnez celles désirées et cliquez sur pour les ajouter dans la liste des amis. Si vous cliquez sur **toutes les adresses** email seront ajoutées à la liste. Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**. Si vous cliquez sur le bouton **Vider la liste** vous supprimerez toutes les entrées de la liste, mais attention : il sera alors impossible de les récupérer. Utilisez les boutons **Sauvegarder/** **Charger** pour sauvegarder/charger la Liste des amis vers un emplacement désiré. Le fichier a l'extension .bwl. Pour supprimer le contenu de la liste en cours d'utilisation quand vous chargez une liste sauvegardée auparavant, choisissez Au chargement, **nettoyer la liste en cours**.



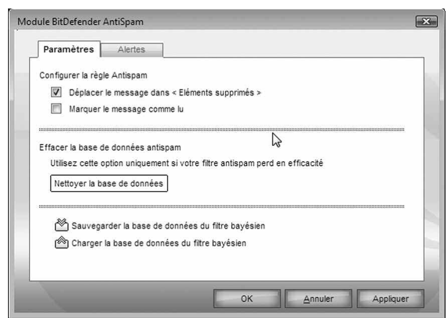
Note

Nous vous suggérons d'ajouter les noms de vos amis et leurs adresses email à la Liste des Amis. BitDefender ne bloque pas les messages provenant de cette liste ; ajouter des amis vous aide à laisser passer les messages légitimes.

Cliquez sur **Appliquer** et **OK** pour sauvegarder et fermer la **liste d'amis.**

- **Configuration** - cliquez ce bouton pour ouvrir le panneau de **Configuration**.

Configuration



Les options suivantes sont disponibles :

- **Déplacer le message dans Eléments supprimés** - déplace les messages spam dans la Corbeille (seulement pour Outlook Express / Windows Mail) ;
- **Marquer le message comme 'lu'** - marque tous les messages spam comme "lus" pour ne pas déranger quand de nouveaux spams arrivent.

Si votre filtre est peu efficace, vous devriez effacer les données du filtre bayesien et le reformer.

Cliquez sur **Effacer la base de données antispam** pour réinitialiser les données du filtre bayesien.

Utilisez les boutons **Sauvegarder les règles du filtre Bayesien/** **Charger les règles du filtre Bayesien** pour sauvegarder / charger la base de données bayésienne vers un emplacement désiré. Le fichier aura une extension .dat.

Cliquez sur l'onglet **Alertes** pour accéder à la rubrique où vous pouvez désactiver l'apparition des fenêtres de confirmation pour **Ajout spammeur** et **Ajout ami**.



Note

Dans la fenêtre Alertes vous pouvez aussi activer/désactiver l'apparition de l'alerte Merci de choisir un email. Cette alerte apparait quand vous choisissez un group au lieu d'un seul email.

- **Assistant** - cliquez dessus pour lancer l'assistant qui vous aidera à former le filtre bayesien, pour accroître l'efficacité de BitDefender Antispam. Vous pouvez aussi ajouter des adresses de votre **carnet d'adresses** dans vos **Listes d'amis / spammeurs.**
- **BitDefender Antispam** - cliquez dessus pour ouvrir la Console de gestion.

9.4.2. Assistant de configuration de l'Antispam

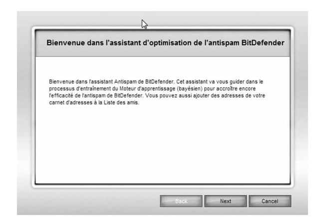
Lors de la première exécution de votre client de messagerie une fois BitDefender installé, un assistant apparaît afin de vous aider à configurer la Liste des amis et la Liste des spammeurs et à entraîner le filtre bayesien afin d'améliorer l'efficacité des filtres antispam.



Note

L'assistant peut également être lancé à tout moment en cliquant sur le bouton Assistant depuis la barre d'outils Antispam

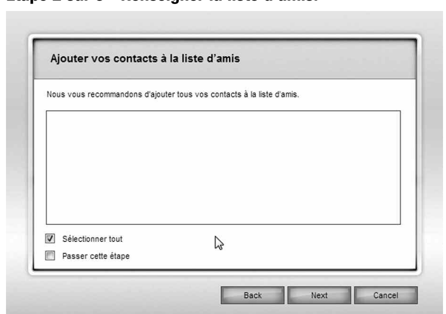
Etape 1 sur 6 – Fenêtre de Bienvenue



Fenêtre d'accueil

Cliquez sur **Suivant**.

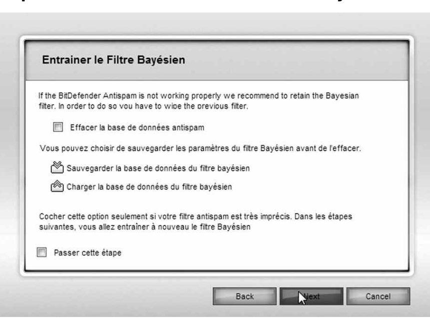
Etape 2 sur 6 - Renseigner la liste d'amis.



Renseigner la liste d'amis

Ici vous pouvez voir toutes les adresses de votre **Carnet d'adresses.** Choisissez ceux que vous désirez ajouter à votre Liste d'amis (nous vous recommandons de toutes les rajouter). Vous allez recevoir tous les messages provenant de ces adresses, quel que soit leur contenu. Choisissez **Passé cette étape** si vous voulez passer sans l'appliquer. Cliquez sur **Précédent** pour revenir ou cliquez sur Suivant pour continuer.

Etape 3 sur 6 - Effacer la base de données bayesienne

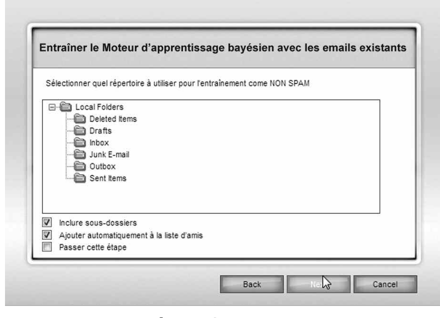


Effacer la base de données bayesienne

Vous pouvez découvrir votre filtre antispam commence à perdre en efficacité. Cela peut être dû à une formation défectueuse (par ex. vous avez rapporté un nombre de messages légitimes comme spam ou l'inverse). Si votre filtre est peu efficace, nous vous conseillons d'effacer les données du filtre bayesien et le reformer suivant les étapes ci-dessous.
Choisir **Effacer la base de données antispam** pour réinitialiser les données du filtre bayesien.

Utilisez les boutons **Sauvegarder Bayesien/ Charger Bayesien** pour sauvegarder / charger la base de données bayésienne vers l'emplacement désiré. Le fichier aura une extension .dat.
Choisissez **Passer cette étape** si vous voulez passer sans l'appliquer. Cliquez sur **Précédent** pour revenir ou cliquez sur Suivant pour continuer.

Etape 4 sur 6 - Entraîner le filtre bayesien avec des messages légitimes



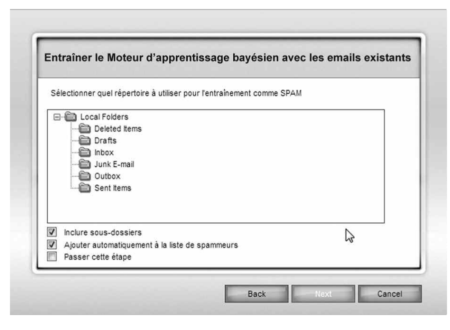
Entraîner le filtre bayesien avec des messages légitimes

Choisissez un dossier contenant des messages légitimes. Ils seront utilisés pour entraîner le filtre antispam.
Deux options apparaissent dans la partie supérieure de la fenêtre :

- **Inclure sous-dossiers** - pour inclure les sous-dossiers dans votre choix ;
- **Ajouter automatiquement à la liste d'amis** - pour ajouter les expéditeurs à la liste d'amis.

Choisissez **Passer cette étape** si vous voulez passer sans l'appliquer. Cliquez sur **Précédent** pour revenir ou cliquez sur **Suivant** pour continuer.

Etape 5 sur 6 - Entraîner le filtre bayesien avec des messages SPAM



Entraîner le filtre bayesien avec des messages SPAM

Choisissez un dossier contenant des messages spam. Ils seront utilisés pour entraîner le filtre antispam.



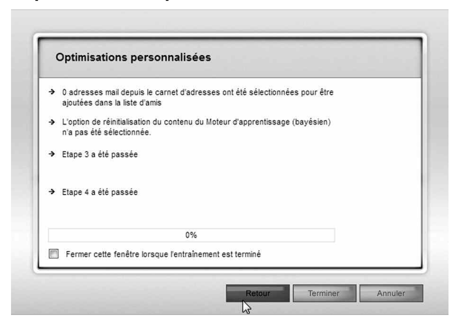
Important
Vérifiez si le dossier choisi ne contient aucun message légitime, sinon la précision de l'antispam se verra considérablement réduite.

Deux options apparaissent dans la partie supérieure de la fenêtre :

- **Inclure sous-dossiers** - pour inclure les sous-dossiers dans votre choix ;
- **Ajouter automatiquement à la liste des spammeurs** - pour ajouter les expéditeurs à la liste des spammeurs.

Choisissez **Passer cette étape** si vous voulez passer sans l'appliquer. Cliquez sur **Précédent** pour revenir ou cliquez sur **Suivant** pour continuer.

Etape 6 sur 6 – Récapitulatif



Récapitulatif

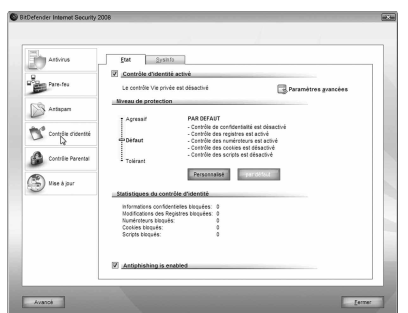
Ici vous pouvez consulter toute les options choisies avec l'assistant de configuration. Vous pouvez opérer des modifications en retournant aux étapes précédentes (cliquez sur **Précédent**). Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

10. Contrôle d'identité

BitDefender contrôle des dizaines de “points à risque” dans votre système où les spywares pourraient agir, et analyse également les modifications apportées à votre système et à vos logiciels. C’est efficace contre les chevaux de Troie et autres outils installés par des hackers, qui essaient de compromettre votre vie privée et d’envoyer vos informations personnelles, comme vos numéros de carte bancaire, de votre ordinateur vers le pirate.
BitDefender peut également analyser les sites Internet que vous visitez et vous alerter si une menace de phishing est détectée.
La section du **contrôle d'identité** de ce manuel d'utilisation contient les sujets suivants :

- Statut du contrôle d'identité
- Paramètres avancés - Contrôle de la vie privée
- Paramètres avancés - Contrôle de la base de registres
- Paramètres avancés - Contrôle des cookies
- Paramètres avancés - Contrôle des scripts
- Information Système
- Barre d'outils Antiphishing

10.1. Statut du contrôle d'identité



Pour configurer le contrôle d'identité et consulter les informations concernant son activité, cliquez sur Statut du contrôle d'identité> dans les paramètres de la console. La fenêtre suivante apparaît :

Statut du contrôle d'identité

10.1.1. Contrôle d'identité



Important
Pour empêcher les spywares d'infecter votre ordinateur, le contrôle d'identité doit rester activé.

Le contrôle d'identité protège votre ordinateur en recourant aux 5 contrôles majeurs de sécurité :

- Controle Vie Privée - protège vos informations confidentielles en filtrant tout le trafic HTTP sortant (pages Web) et SMTP (emails) selon les règles crées dans la rubrique Vie privée
- Contrôle de la base de registres - demande votre autorisation quand un programme tente de modifier la base de registres pour être exécuté au démarrage de Windows.
- Contrôle des cookies - demande votre autorisation quand un nouveau site Internet tente de déposer un cookie sur votre ordinateur.
- Contrôle des scripts - demande votre autorisation quand un site Internet tente d'activer un script ou tout autre contenu actif.

Pour configurer les paramètres de ces contrôles, cliquez sur **Paramètres avancés.**
En bas de la section, vous pouvez consulter les statistiques concernant le contrôle d'identité.
Configuration du niveau de protection
Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection :

Niveau de protection	Description
Tolérant	Seul le Contrôle de la base de registre est activé.
Défault	Le Contrôle de la base de registre et le Contrôle vie privée sont activés.
Agressif	Le Contrôle de la base de registre, le Contrôle Vie privée et le module d'analyse de script sont activés. Vous pouvez personnaliser le niveau de protection en cliquant sur Niveau de personnalisation. Sélectionnez dans la fenêtre apparue les contrôles Antispyware que vous désirez activer et cliquez sur OK. Cliquez sur Niveau par défaut pour placer le curseur sur le niveau par défaut.

10.1.2. Protection antiphishing

Le phishing est une activité criminelle pratiquée sur Internet qui repose sur les techniques d'ingénierie sociale ; son but est de piéger des personnes afin de leur soutirer des renseignements d'ordre personnel. La plupart du temps, les tentatives de phishing se traduisent par l'envoi massif d'emails qui prétendent émaner d'une société digne de confiance. Ces faux messages sont envoyés dans l'espoir que quelques-uns des destinataires qui correspondent au profil de la cible du phishing divulgueront alors des renseignements d'ordre personnel.

En règle générale, un message de phishing signale un problème avec votre compte en ligne. Il vous invite à cliquer sur un lien fourni dans le message pour accéder à un site Web supposé authentique (en fait un site frauduleux) où des renseignements d'ordre privé vous sont ensuite demandés. On peut par exemple vous demander de confirmer vos identifiants de connexion à votre compte, c'est-à-dire votre nom d'utilisateur et votre mot de passe, et de fournir vos coordonnées bancaires ou votre numéro de sécurité sociale. Une approche encore plus convaincante consiste à vous faire croire que votre compte a déjà été ou risque d'être suspendu si vous ne cliquez pas sur le lien fourni.

Le phishing utilise également les spywares, tels que des keyloggers introduits par un cheval de Troie, pour dérober des informations concernant votre compte directement au sein de votre ordinateur.

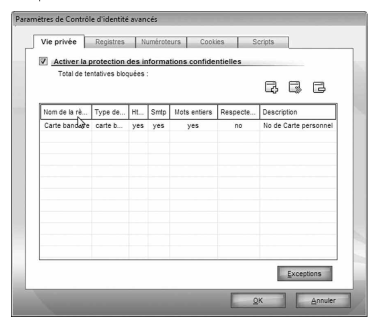
Les principales cibles du phishing sont les clients de services de paiement en ligne, comme eBay et PayPal, ainsi que les banques qui proposent des prestations en ligne. Récemment, les utilisateurs de sites de réseau communautaire (Myspace, etc.) ont également fait l'objet de tentatives de phishing pour obtenir des renseignements d'ordre privé et usurper ensuite leur identité.

Pour vous prémunir contre les tentatives de phishing lors de votre navigation sur Internet, l'antiphishing doit être activé. Ainsi, BitDefender analysera chaque site Internet avant que vous y accédiez et il vous alertera en cas de menaces de phishing. Il est possible de configurer une liste blanche de sites Internet qui ne seront pas analysés par BitDefender.

Afin de gérer facilement la protection antiphishing et la liste blanche, utilisez la barre d'outils antiphishing BitDefender intégrée à Internet Explorer. Pour plus d'informations, reportez-vous à “**Barre d'outils antiphishing**” (p. 121).

10.2. Protection de la vie privée - Paramètres avancés.

La protection des données confidentielles est un sujet important qui nous concerne tous. Le vol d'informations a suivi le développement de l'Internet et des communications et utilise de nouvelles méthodes pour pousser les gens à communiquer leurs données privées. Qu'il s'agisse de votre adresse email ou de votre numéro de carte bancaire, si ces informations tombent dans de mauvaises mains vous pouvez en subir les conséquences : crouler sous le spam ou retrouver votre compte bancaire vide.



Le module **Protection de la vie privée** vous aide à garder vos informations en sécurité. Il analyse le trafic HTTP et SMTP à la recherche des séquences de caractères que vous avez définies et bloque les emails ou les pages Web si il les trouve.
Le support multi-utilisateurs fourni empêche les autres utilisateurs du système d'accéder aux règles que vous avez configurées.
Les règles de confidentialité peuvent être configurées dans la section **Confidentialité**. Pour accéder à cette section, ouvrez la fenêtre des **Paramètres avancés de contrôle d'identité** et cliquez sur l'onglet **Confidentialité**.



Note
Pour ouvrir la fenêtre des Paramètres avancés de contrôle de l'identité, cliquez sur Statut du contrôle d'identité>dans la console des paramètres et cliquez sur Paramètres avancés.

10.2.1. Création de règles de confidentialité

Les règles doivent être entrées manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra. L'assistant de configuration contient 3 étapes.

Etape 1 sur 3 - Définition des types de règles et de données



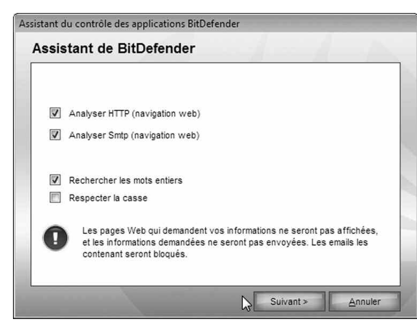
Définition des types de règles et de données
Entrez le nom de la règle dans le champ correspondant.
Vous devez définir les paramètres suivants :
- **Type de règle** - détermine le type de règle (adresse, nom, carte de crédit, code PIN, etc.)
- **Données de la règle** - Renseigner les données de la règle.



Note
Si vous saisissez moins de trois caractères, vous serez invité à valider les données. Nous vous recommandons de saisir au moins trois caractères afin d'éviter le blocage erroné de messages et de pages Web.

Toutes les données que vous enregistrez sont cryptées.

Cliquez sur **Suivant**.



Etape 2 sur 3 - Sélection du trafic

Sélection du trafic

Sélectionnez le type de trafic que BitDefender doit analyser. Les options suivantes sont disponibles :

- **Analyse HTTP** - Analyse le flux HTTP (web) et bloque les données qui sont prévues dans la règle de gestion des données.
- **Analyse SMTP** - Analyse le flux SMTP (mail) et bloque les emails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

Vous pouvez choisir d'appliquer la règle uniquement si les données de la règle correspondent à tous les mots ou à la chaîne de caractères détectée.
Cliquez sur **Suivant**.

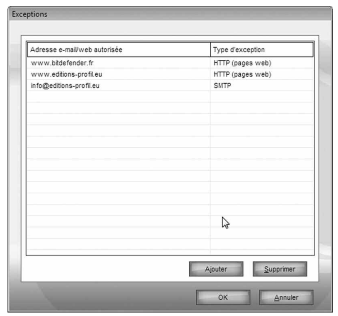
Etape 3 sur 3 – Description de la règle

Description de la règle

Entrez une description courte de la règle dans le champ correspondant.
Cliquez sur **Terminer**.

10.2.2. Définition des exceptions

Il peut arriver de devoir définir des exceptions à des règles de confidentialité spécifiques. Si vous créez, par exemple, une règle de confidentialité pour éviter que votre numéro de carte de crédit ne soit envoyé via HTTP (Web), chaque fois que le numéro de votre carte sera soumis sur un site Web depuis votre compte utilisateur, la page correspondante sera bloquée. Si vous voulez, par exemple, acheter des chaussures sur une boutique en ligne (que vous savez fiable), vous devrez spécifier une exception à la règle correspondante. Pour ouvrir la fenêtre permettant de gérer les exceptions, cliquez sur **Exceptions**.



Exceptions

Pour ajouter une exception, procédez comme suit :

1. Cliquez sur **Ajouter** pour ajouter une nouvelle entrée dans le tableau.
2. Double-cliquez sur S**pécifier adresse autorisée** et indiquez l'adresse Web ou l'adresse e-mail que vous souhaitez ajouter en tant qu'exception.
3. Double-cliquez sur **Choisissez un type** et sélectionnez dans le menu l'option correspondant au type d'adresse précédemment indiquée.

- Si vous avez indiqué une adresse Web, sélectionnez HTTP.
- Si vous avez indiqué une adresse e-mail, sélectionnez SMTP.

Pour supprimer une exception de la liste, sélectionnez-la, puis cliquez sur **Supprimer**.
Cliquez sur **OK** pour sauvegarder les changements.

10.2.3. Gestion des règles



Vous pouvez voir les règles existantes dans le tableau correspondant.

Pour supprimer un règle, sélectionnez-la et cliquez sur le bouton **Effacer**. Pour désactiver temporairement une règle sans pour autant la supprimer, décochez la case correspondante.

Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton **Éditer** ou double-cliquez dessus. Une nouvelle fenêtre est alors affichée.

Dans cette rubrique, vous pouvez modifier le nom, la description et les paramètres de la règle (type, données et trafic). Cliquez sur OK pour enregistrer les modifications.
Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

10.3. Contrôle de la base de registre -Paramètres avancés

Une partie très importante du système d'exploitation Windows est appelée la **Base de registres.** C'est l'endroit où Windows conserve ses paramétrages, programmes installés, informations sur l'utilisateur et autres. La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. Cette fonction est souvent détournée par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le Contrôle des registres surveille les registres Windows – cette fonction est également utile pour détecter des chevaux de Troie. Il vous alertera dès qu'un programme essaiera de modifier une entrée dans la base de registres afin de s'exécuter au démarrage de Windows.



Alerte registres

Vous pouvez refuser cette modification en cliquant sur **Non** ou l'autoriser en cliquant sur **Oui**.
Si vous souhaitez que BitDefender se souvienne de votre réponse, cochez la case **Toujours appliquer cette action pour ce programme.**
Une règle est alors générée et la même action sera appliquée à chaque fois que ce programme tentera de modifier une entrée du registre à exécuter au démarrage de Windows.

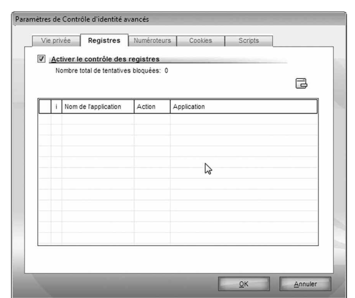


Note
BitDefender vous alertera lors de l'installation de nouveaux logiciels nécessitant d'être lancés après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.

Il est possible d'accéder à chaque règle qui a été traitée dans la section **Registre** pour peaufiner les réglages. Pour accéder à cette section, ouvrez la fenêtre des **Paramètres avancés de contrôle d'identité** et cliquez sur l'onglet **Registre**.



Note
Pour ouvrir la fenêtre des Paramètres avancés de contrôle de l'identité, cliquez sur Statut du contrôle d'identité>dans la console des paramètres et cliquez sur Paramètres avancés.



Contrôle de la base de registre

Vous pouvez voir les règles existantes dans le tableau correspondant.

Pour supprimer une règle, il suffit de la sélectionner et de cliquer sur le bouton **Effacer la règle**. Pour supprimer toutes les règles, cliquez sur le bouton Nettoyer liste. Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton **Éditer**
la règle ou double-cliquez dessus. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante. Pour désactiver temporairement une option sans l'effacer, décochez la case correspondante.
Pour modifier l'action d'une règle, double-cliquez sur le champ de l'action et sélectionnez l'option correspondante dans le menu.
Cliquez sur **OK** pour fermer la fenêtre.

10.4. Contrôle des cookies - Paramètres avancés

Les Cookies sont très communs sur Internet. Ce sont des petits fichiers stockés sur l'ordinateur. Les sites web les créent afin de connaître certaines informations concernant vos habitudes de surf.

Les Cookies sont généralement là pour vous faciliter la navigation. Par exemple, ils peuvent permettre à un site web de mémoriser votre nom et vos préférences, pour que vous n'ayez pas à les renseigner à nouveau. Mais les cookies peuvent aussi être utilisés pour compromettre la confidentialité de vos données, en surveillant vos préférences de navigation. C'est là que la fonction **Contrôle des cookies** est très utile. Si elle est activée, la fonction Contrôle des cookies vous demandera une validation à chaque fois qu'un nouveau site Web tentera de déposer un cookie.



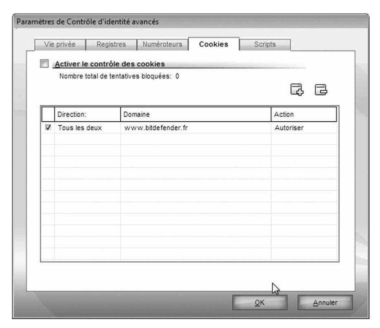
Alerte de cookies
Vous pouvez voir le nom de l'application qui tente d'envoyer un fichier de type cookie.
Sélectionnez **Retenir cette réponse** et cliquez sur **Oui** ou **Non** et une règle sera créée, appliquée et listée dans le tableau des règles.
Cette fonction vous aide à choisir à quels sites faire confiance et quels sites vous préférez éviter.

Note
A cause du grand nombre de cookies utilisés sur Internet, le module Contrôle des Cookies peut être légèrement gênant au départ. Il vous posera beaucoup de questions concernant l'acceptation de nouveaux cookies sur votre ordinateur. Au fur et à mesure que vous ajouterez vos sites Web favoris à la liste des règles, votre navigation redeviendra aussi simple qu'auparavant.

Vous pouvez éditer chaque règle mémorisée dans la section **Cookie** pour y apporter des modifications.
Pour accéder à cette section, ouvrez la fenêtre des **Paramètres antispyware avancés** et cliquez sur l'onglet Cookie.



Note
Pour ouvrir a fenêtre des Paramètres antispyware avancés, cliquez sur Statut du contrôle d'identité> dans la console des paramètres et cliquez sur Paramètres avancés.



Contrôle des cookies
Vous pouvez voir les règles existantes dans le tableau correspondant.



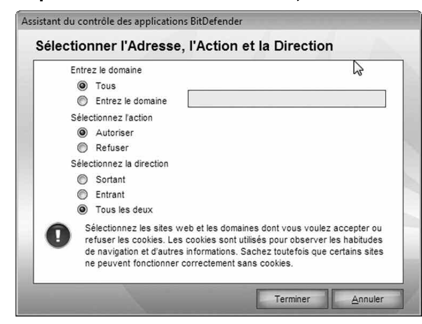
Important
Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez la et cliquez sur le bouton **Effacer**. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faîtes la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante. Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

10.4.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1 sur 1 - Sélection de l'Adresse, de l'Action et de la Direction



Sélection de l'Adresse, de l'Action et de la Direction

Vous pouvez définir les paramètres :

- **Adresse domaine** - vous pouvez introduire le nom de domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action liée à la règle.
- Direction - sélectionne la direction du trafic.

Autoriser :	Les cookies de ce domaine seront autorisés.
Interdire :	Les cookies de ce domaine ne seront pas autorisés.
Sortant :	La règle s'applique seulement aux envois d'informations vers les serveurs auxquels vous accédez.
Entrant :	La règle s'applique seulement aux envois d'informations en provenance des serveurs auxquels vous accédez.
Les deux :	La règle s'applique dans les deux directions.

Cliquez sur **Terminer**.



Note
Vous pouvez accepter des cookies et interdire leur envoi en sélectionnant l'action Interdire et la direction Sortant.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

10.5. Contrôle des scripts - Paramètres avancés

Les Scripts et d'autres codes comme les contrôles ActiveX et Applets Java, qui sont utilisés pour créer des pages web interactives, peuvent être programmés pour avoir des effets néfastes. Les éléments ActiveX, par exemple, peuvent obtenir un accès total à vos données et peuvent lire des données depuis votre ordinateur, supprimer des informations, capturer des mots de passe et intercepter des messages lorsque vous êtes en ligne. Il est recommandé de n'accepter les contenus actifs que sur les sites que vous connaissez et auxquels vous faites parfaitement confiance. BitDefender vous laisse le choix d'exécuter ou de bloquer ces éléments. Avec le Contrôle de scripts vous pourrez définir les sites web auxquels vous faites confiance ou non. BitDefender vous demandera une validation dès qu'un site web essaiera d'activer un script ou tout type de contenu actif :

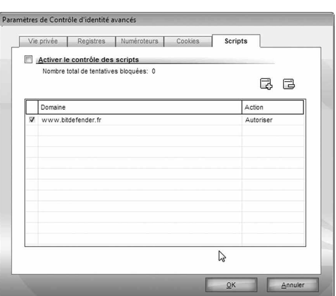


Alerte de scripts

Vous pouvez voir le nom de la ressource. Sélectionnez Retenir cette réponse et cliquez sur Oui ou Non et une règle sera créée, appliquée et listée dans le tableau des règles. Vous ne serez dès lors plus interrogé lorsque ce même site essaiera de vous envoyer un contenu actif.
Chaque règle mémorisée peut être éditée dans la partie Scripts pour y apporter des modifications. Pour accéder à cette section, ouvrez la fenêtre des Paramètres avancés de contrôle d'identité et cliquez sur l'onglet Script.



Note
Pour ouvrir la fenêtre des Paramètres avancés de contrôle de l'identité, cliquez sur Statut du contrôle d'identité>dans la console des paramètres et cliquez sur ***Paramètres avancés****.*



Contrôle des scripts
Vous pouvez voir les règles existantes dans le tableau correspondant.



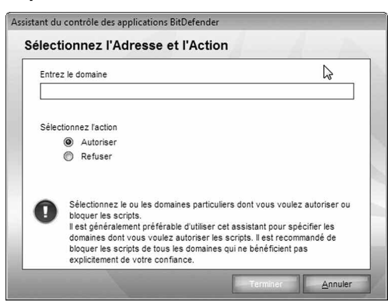
Important
Les règles sont listées dans l'ordre de priorité en commençant par le haut de la liste, la première règle a la priorité la plus élevée. Glisser & déposer les règles afin de changer leur priorité.

Pour supprimer une règle, sélectionnez la et cliquez sur le bouton Effacer. Pour modifier les paramètres d'une règle, double-cliquez sur son champ et faîtes la modification souhaitée. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.
Les règles peuvent être entrées automatiquement (via la fenêtre d'alerte) ou manuellement (cliquez sur le bouton **Ajouter** et choisissez les paramètres de la règle). L'assistant de configuration apparaîtra.

10.5.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1 sur 1 - Sélection des adresses de domaine et Action



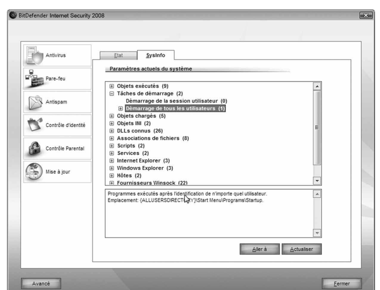
Sélection des adresses de domaine et Action
Vous pouvez définir les paramètres :
- **Adresse domaine** - vous pouvez introduire le nom de domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action liée à la règle.

Autoriser :	Les scripts de ce domaine seront exécutés.
Interdire :	Les scripts de ce domaine ne seront pas exécutés.

Cliquez sur **Terminer**.
Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

10.6. Informations Système

BitDefender vous permet d'afficher, à partir d'un emplacement unique, tous les paramètres du système ainsi que les applications enregistrées pour être exécutées au démarrage. Vous pouvez ainsi contrôler l'activité du système et des applications installées et identifier d'éventuelles infections. Pour obtenir des informations sur le système, cliquez sur **Informations système contrôle d'identité**> dans les paramètres de la console. La fenêtre suivante apparaît :



Informations Système
La liste contient tous les éléments chargés au démarrage du système ainsi que les ceux chargés par les différentes applications.
Trois boutons sont disponibles :
- Retirer - supprime les objets sélectionnés. Vous devez cliquer sur Oui pour confirmer votre choix.



Note
Si vous ne souhaitez plus être invité à confirmer votre choix lors de la session en cours, cochez la case Ne plus me poser la question pendant cette session.

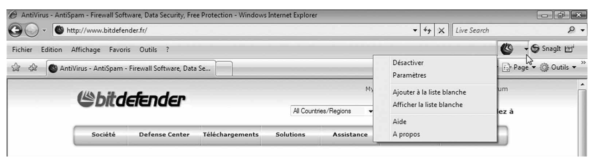
- **Aller à** - ouvre une fenêtre dans laquelle l'objet a été placé (la Base de Registres par exemple).
- **Actualiser** - re-ouvre la rubrique Informations système.

10.7. Barre d'outils antiphishing

BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet. Il analyse les sites Web auxquels vous accédez et vous prévient en cas de menaces de phishing. Il est possible de configurer une liste blanche de sites Internet qui ne seront pas analysés par BitDefender.
La barre d'outils antiphishing BitDefender intégrée à Internet Explorer vous permet de gérer facilement et efficacement la protection antiphishing et la liste blanche.
La barre d'outils antiphishing, représentée par **l'icône BitDefender** , est située en haut de la fenêtre d'Internet Explorer. Cliquez dessus pour ouvrir le menu de la barre d'outils.



Note
Si vous ne voyez pas la barre d'outils, cliquez sur le menu Affichage, sélectionnez Barres d'outils et vérifiez que la barre d'outils BitDefender y figure bien.



Barre d'outils antiphishing
Les commandes suivantes sont disponibles dans le menu de la barre d'outils :
• Activer / Désactiver - active / désactive la barre d'outils antiphishing BitDefender.



Note
Si vous choisissez de désactiver la barre d'outils antiphishing, votre ordinateur ne sera plus protégé contre les tentatives de phishing.

• Paramètres - ouvre une fenêtre où vous pouvez préciser les paramètres de la barre d'outils antiphishing.

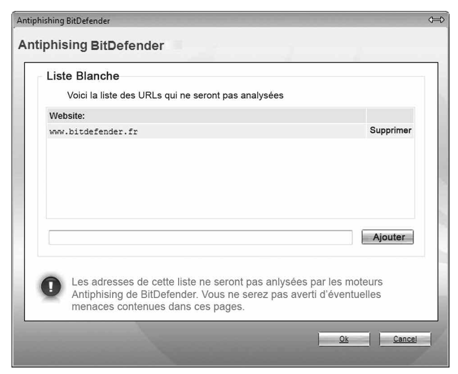


Paramètres de la barre d'outils Antiphishing
Les options suivantes sont disponibles :
• Activation de l'analyse- Activation de l'analyse antiphishing.
• Demander avant d'ajouter à une liste blanche - Demande d'autorisation pour ajouter un site Web à la liste blanche.
• Ajouter à la liste blanche - Ajout du site Web actuel à la liste blanche.



Note
Si vous ajoutez un site Web à la liste blanche, BitDefender n'analysera plus le site pour détecter les tentatives de phishing. Nous vous recommandons d'ajouter uniquement à la liste blanche les sites auxquels vous faites pleinement confiance.

• Afficher la liste blanche - Ouverture de la liste blanche.



Liste blanche antiphishing

Vous pouvez consulter la liste de tous les sites Web qui ne seront pas analysés par les moteurs BitDefender d'antiphishing.
Si vous souhaitez **supprimer** un site de la liste blanche – pour pouvoir être prévenu de tout risque de phishing sur la page correspondante, cliquez sur le bouton Supprimer en regard du nom du site.
Vous pouvez ajouter à la liste blanche les sites auxquels vous faites pleinement confiance, pour qu'ils ne soient plus analysés par les moteurs d'antiphishing. Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur le bouton Ajouter.
• **Aide** - ouvre la documentation d'aide électronique.
• **A propos de** - Affichage d'une fenêtre contenant des informations relatives à BitDefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.

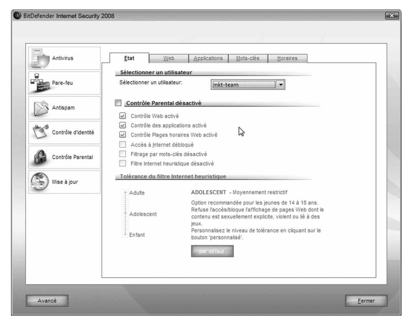
11. Contrôle Parental

Le module de Contrôle Parental de BitDefender peut bloquer l'accès à des sites web que vous considérez inappropriés, bloquer l'accès à Internet pour une certaine période de temps (par exemple lorsqu'il est l'heure pour les leçons), et bloquer des applications comme des jeux, chat, programmes d'échange de fichiers ou autres.

Important
Ce module n'est accessible qu'aux utilisateurs disposant de droits administrateur. Il peut être nécessaire d'entrer un mot de passe pour y accéder. NB : Un administrateur ne peut pas implémenter un nouveau jeu de règles pour un utilisateur si un autre administrateur l'a déjà fait. Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres BitDefender par un mot de passe. Pour définir un mot de passe, cliquez sur Avancé dans la console des paramètres et utilisez l'option Activer la protection par mot de passe des paramètres du produit.

Le chapitre **Contrôle Parental** de ce guide utilisateur contient les rubriques suivantes :
- Etat du Contrôle Parental
- Contrôle web
- Contrôle des Programmes
- Filtrage des mots clés
- Plages horaires Web

11.1. Etat du Contrôle Parental



Pour configurer le contrôle parental pour un utilisateur sélectionné, cliquez sur **Contrôle parental > État** dans la console des paramètres. La fenêtre suivante apparaît :

Etat du Contrôle Parental



Important
Laissez le Contrôle parental actif pour protéger vos enfants contre les contenus inappropriés en utilisant les droits d'accès personnalisés à l'ordinateur.

11.1.1. Sélection des contrôles de protection

Afin de paramétrer le niveau de protection vous devez d'abord choisir à quel utilisateur il s'appliquera. Puis, configurez le niveau de protection en utilisant les contrôles suivants :

- **Contrôle Web** - active le Contrôle Web pour filtrer la navigation Internet en fonction des règles que vous avez définies dans la partie Web.
- **Contrôle des applications** - activez le Contrôle des applications afin de bloquer l'accès aux applications que vous avez déterminées dans la partie Applications.
- **Planificateur d'utilisation Internet** - activez le Planificateur d'utilisation Internet pour accorder un accès Internet selon les critères que vous avez déterminés dans la partie Planificateur d'utilisation Internet.
- Cliquez sur **Bloquer** pour bloquer l'accès à l'ensemble des sites web (et pas uniquement ceux de la section Web).
- **Filtre de mots clés** - activez le Filtre de mots clés pour filtrer l'accès au Web et aux emails en fonction des règles que vous avez définies dans le module Mots Clés.
- Filtre Internet heuristique - activez cette option pour filtrer l'accès à Internet en fonction des règles pré-établies selon les catégories d'âge.



Note
Pour profiter pleinement des fonctions proposées par le contrôle parental, vous devez configurer les contrôles sélectionnés.

11.1.2. Configuration du filtre Internet heuristique

Le filtre Internet heuristique analyse les pages Web et bloque celles qui correspondent aux caractéristiques d'un contenu potentiellement inapproprié. Vous pouvez définir un niveau de protection en utilisant des jeux de règles prédéfinis basés sur l'âge pour filtrer l'accès Web ou vous pouvez sélectionner des catégories de contenu dont vous souhaitez bloquer l'accès.

Déplacez le curseur sur l'échelle graduée et choisissez le niveau de protection qui vous semble approprié pour l'utilisateur concerné.

Il existe trois niveaux de protection :

Enfant : Offre un accès limité au Web selon les critères sélectionnés pour un utilisateur de moins de 14 ans. Les pages Web au contenu potentiellement nuisible pour les enfants (pornographie, sexualité, drogue, hacking, etc.) sont bloquées.

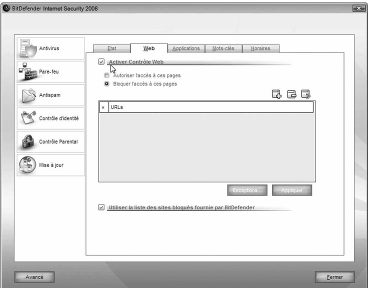
Adolescent : Offre un accès restreint à Internet en prenant en compte les paramètres recommandés pour des utilisateurs ayant entre 14 et 18 ans. Les pages Web ayant un contenu sexuel, pornographique ou pour adulte sont bloquées.

Adulte : Offre un accès illimité à toutes les pages Web quel que soit leur contenu.

Cliquez sur **Niveau personnalisé** pour définir vos propres règles de filtrage. Dans la fenêtre qui s'affiche, sélectionnez les catégories de contenus (jeux d'argent, piratage, pornographie, etc.) dont vous souhaitez que BitDefender bloque l'accès, puis cliquez sur OK.
Cliquez sur **par défaut** pour placer le curseur sur le niveau par défaut.

11.2. Contrôle Web

Le **Contrôle Web** vous aide à bloquer l'accès à des sites Internet ayant un contenu inapproprié. La liste de sites interdits sera actualisée par BitDefender, durant le processus de mise à jour habituel. Les pages contenant des références (ou des liens) à des sites interdits peuvent également être bloqués. Pour configurer le contrôle Web, cliquez sur **Contrôle parental > Web** dans la console des paramètres.
La fenêtre suivante apparaît :



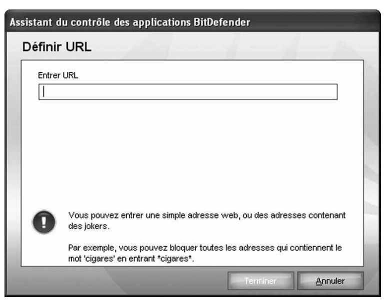
Contrôle Web

Pour activer cette protection, sélectionnez-la case correspondant à la fonction **Activer Contrôle Web.** Sélectionnez **Autoriser** l'accès à ces pages/Bloquer l'accès à ces pages pour voir la liste des sites autorisés/bloqués. Cliquez sur Exceptions... pour accéder à la liste complémentaire. Les règles doivent être entrées manuellement. Tout d'abord, choisissez un des options : Autoriser l'accès à ces pages/Bloquer l'accès à ces pages pour autoriser/bloquer l'accès aux sites web que vous spécifierez dans l'assistant. Ensuite, cliquez sur le bouton **Ajouter**... pour démarrer l'assistant de configuration.

11.2.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1/1 – Sélectionner les sites web



Sélectionner les sites web
Tapez le nom du site web pour lequel la règle sera appliquée et cliquez sur Terminer.



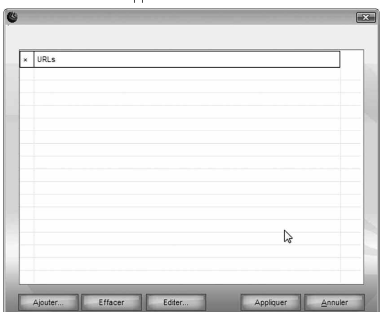
Important
Syntaxe :
• *.xxx.com - l'action de la règle s'appliquera à l'ensemble des sites web se terminant par .xxx.com ;
• *porn* - l'action de la règle s'appliquera à l'ensemble des sites web contenant <porn> dans son adresse web ;
• www.*.com - l'action de la règle s'appliquera à l'ensemble des sites web ayant comme suffixe de domaine com.
• www.xxx.* - l'action de la règle s'appliquera à l'ensemble des sites web commençant par www.xxx., quelque soit le suffixe du nom de domaine.

N'oubliez pas de cliquer sur **Appliquer** pour enregistrer vos modifications.
Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Effacer**. Pour modifier une règle, sélectionnez-la et cliquez sur le bouton **Editer**... ou double-cliquez sur la règle. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

11.2.2. Choisir des exceptions

Vous pouvez parfois avoir besoin de créer des exceptions à certaines règles. Par exemple, vous avez défini une règle qui bloque les sites contenant le mot "killer" dans leur adresse (syntax : *killer*).Vous avez également connaissance d'un site nommé "killer-music" sur lequel les visiteurs peuvent écouter de la musique en ligne. Pour créer une exception à la règle, accédez à la fenêtre Exceptions et définissez une exception à la règle.
Cliquez sur Exceptions....

La fenêtre suivante apparaîtra :



Choisir des exceptions

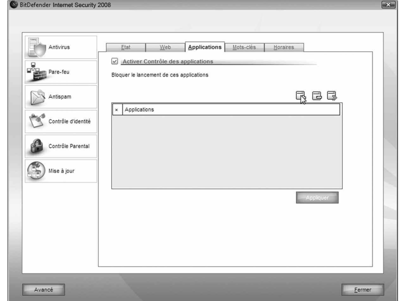
Cliquez sur **Ajouter**...pour déterminer les exceptions. L'assistant de configuration apparaîtra pour vous aider à définir les exceptions.
N'oubliez pas de cliquer sur Appliquer pour enregistrer vos modifications.
Pour effacer une règle, sélectionner-la et cliquez sur Effacer. Pour modifier une règle, sélectionnez-la et cliquez sur Editer ou double-cliquez dessus. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

11.2.3. Liste noire Web de BitDefender

Pour vous aider à protéger vos enfants contre les contenus Web inappropriés, BitDefender dispose d'une liste noire de sites bloqués. Pour bloquer les sites contenus dans cette liste, sélectionnez Utilisez la liste de sites bloqués par BitDefender.

11.3. Contrôle des Applications

Le **Contrôle des Programmes** vous aide à bloquer des applications. Jeux, logiciel de messagerie, ou toute autre catégorie de logiciels et malware peuvent également être bloqués de cette façon. Les applications bloquées de cette manière sont de plus protégées contre toutes les modifications et ne peuvent pas être copiées ou déplacées.
Pour configurer le contrôle des applications, cliquez sur **Contrôle parental > Applications** dans la console des paramètres. La fenêtre suivante apparaît :



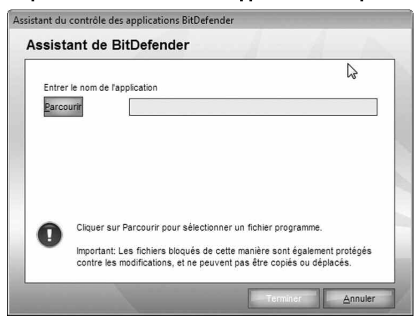
Contrôle des Applications

Pour activer cette protection, sélectionnez la case correspondante **Activer Contrôle des Programmes.** Les règles doivent être entrées manuellement. Cliquez sur le bouton **Ajouter**... pour démarrer l'assistant de configuration.

11.3.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1 sur 1 – Sélection de l'application à bloquer

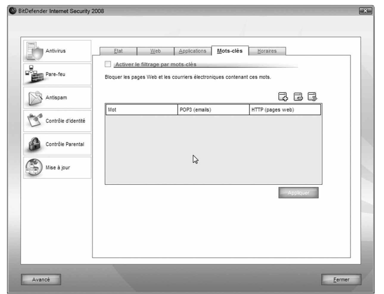


Sélection de l'application à bloquer

Cliquez sur **Explorer**, sélectionnez l'application à bloquer et cliquez sur **Terminer**.
N'oubliez pas de cliquer sur **Appliquer** pour enregistrer vos modifications.
Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Effacer**. Pour modifier une règle, sélectionnez-la et cliquez sur le bouton **Editer**... ou double-cliquez sur la règle. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

11.4. Filtrage de mots clés

Le filtre de mots clés vous aide à bloquer l'accès aux emails et pages Web qui contiennent des mots spécifiques. Vous pouvez ainsi empêcher les utilisateurs de voir des mots ou phrases inappropriées.
Pour configurer le filtrage par mots-clés, cliquez sur **Contrôle parental > Mots-clés** dans la console des paramètres. La fenêtre suivante apparaît :



Filtrage de mots clés

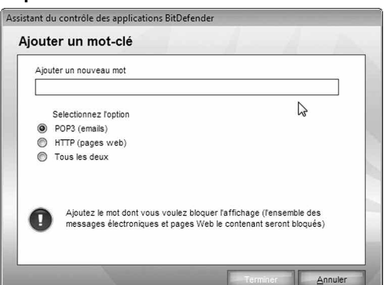
Pour activer cette protection, sélectionnez la case correspondante Filtrage des mots clés.

Les règles doivent être entrées manuellement. Cliquez sur le bouton **Ajouter**... pour démarrer l'assistant de configuration.

11.4.1. Assistant de configuration

L'assistant de configuration ne comporte qu'une seule étape.

Etape 1/1 - Entrez les mots clés



Choix des Mots clés

Vous devez définir les paramètres suivants :

- Mots clés - entrez dans le champ prévu le mot ou la phrase que vous voulez bloquer.
- Protocole - choisissez le protocole (POP, HTTP) que BitDefender doit analyser pour le mot choisi.

Les options suivantes sont disponibles :

POP3 :	Les emails qui contiennent le mot clé sont bloqués.
HTTP :	Les pages Web qui contiennent le mot clé sont bloquées
Les deux :	Les emails et les pages Web qui contiennent le mot clé sont bloqués

N'oubliez pas de cliquer sur Appliquer pour enregistrer vos modifications.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Effacer**. Pour modifier une règle, sélectionnez-la et cliquez sur le bouton **Editer**... ou double-cliquez sur la règle. Pour désactiver temporairement une règle sans la supprimer, décochez la case correspondante.

11.5. Planificateur horaire Web

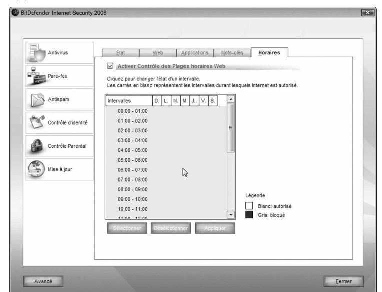
Les Plages horaires web vous permettent d'autoriser ou d'interdire l'accès à Internet pour des utilisateurs ou des applications durant une période de temps donnée.



Note

BitDefender réalisera des mises à jour toutes les heures quelque soit les paramètres des Plages horaires web.

Pour configurer le contrôle des plages horaires Web, cliquez sur **Contrôle parental > Horaires dans la console des paramètres**. La fenêtre suivante apparaît :



Planificateur horaire Web

Pour activer cette protection, sélectionnez la case correspondante **Activer contrôle des plages horaires Web.**

Sélectionnez la durée pendant laquelle les connexions Internet seront bloquées. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures, ou vous pouvez cliquez sur plus de cellules pour bloquer de plus longues périodes. Vous pouvez également cliquer sur **Tout sélectionner** ce qui bloquera implicitement la totalité de l'accès à Internet. Si vous cliquez Tout désélectionner, la connexion à Internet sera toujours autorisée.



Important

Les cases grises représentent les périodes durant lesquelles les connexions Internet seront bloquées.

N'oubliez pas de cliquer sur **Appliquer** pour enregistrer vos modifications.

12. Mise à jour

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important que BitDefender soit à jour dans les signatures de codes malveillants.
Si vous êtes connecté à Internet par câble ou xDSL, BitDefender s'en occupera automatiquement. Il lance la procédure de mise à jour de la base virale à chaque fois que vous démarrez votre ordinateur puis toutes les heures.
Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de mise à jour automatique. Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.
La rubrique Mise à jour de ce Manuel d'utilisation contient les thèmes suivants :

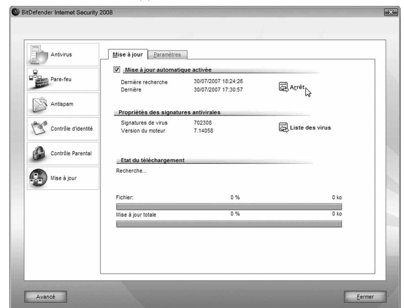
- **Mise à jour des moteurs antivirus** - comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de Virus Definitions Update.
- **Mise à jour pour le moteur antispam** - de nouvelles règles seront ajoutées aux filtres heuristique et URL et de nouvelles images seront ajoutées au filtre d'images. Cela augmentera l'efficacité de votre moteur Antispam. Elles s'affichent sous le nom de Antispam Update.
- **Mise à jour des moteurs antispyware** - de nouvelles signatures seront ajoutées à la base de données. Elles s'affichent sous le nom de Spyware Definitions Update.
- **Mise à jour produit** - lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de Product Update.

Le chapitre Mise à jour de ce manuel d'utilisation contient les thèmes suivants :

- **Mise à jour automatique**
- **Paramètres de mise à jour**

12.1. Mise à jour automatique

Pour afficher des informations sur les mises à jour et exécuter des mises à jour automatiques, cliquez sur Mise à jour > Mise à jour dans la console des paramètres.
La fenêtre suivante apparaît :



Mise à jour automatique

C'est ici que vous pouvez consulter la date de la dernière recherche de mises à jour et celle de la dernière mise à jour, ainsi que des informations sur la dernière mise à jour effectuée (ou les erreurs rencontrées). Sont également affichées des informations sur la version actuelle du moteur de recherche et le nombre de signatures.
Vous pouvez accéder aux signatures de codes malveillants de votre application BitDefender en cliquant sur Liste des virus. Un fichier HTML contenant toutes les signatures disponibles est créé et s'ouvre dans un navigateur Web. Vous pouvez rechercher dans la base de données une signature de code malveillant spécifique ou cliquez sur **Liste des virus BitDefender** pour accéder à la base de données en ligne des signatures BitDefender.
Si vous ouvrez cette section pendant une mise à jour, vous pourrez accéder à l'état du téléchargement.



Important
Pour être protégé contre les dernières menaces, il est impératif de laisser la mise à jour automatique active.

12.1.1. Demandes de mise à jour

Le module **Mise à jour** se connecte au serveur de mise à jour BitDefender et recherche les mises à jour disponibles. Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de la mise à jour manuelle.

Le module Mise à jour se connecter au serveur de mise à jour BitDefender et recherche les mises à jour disponibles. Si une mise à jour est détectée, vous serez invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de la mise à jour manuelle.



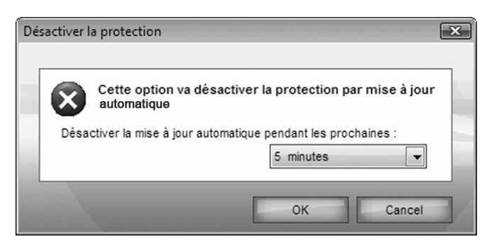
Important
Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible pour bénéficier de la meilleure protection disponible.



Note
Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande.

12.1.2. Désactiver la mise à jour automatique

Si vous tentez de désactiver la mise à jour automatique, une fenêtre d'avertissement apparaît.



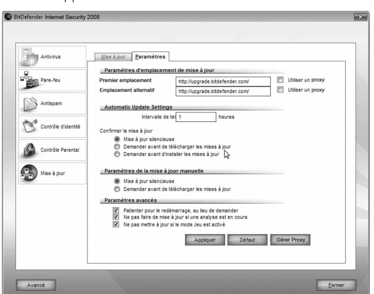
Désactiver la mise à jour automatique
Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la mise à
jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.



Avertissement
Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la mise à jour automatique pendant le moins de temps possible. Si BitDefender n'est pas régulièrement mis à jour, il ne pourra pas vous protéger contre les dernières menaces.

12.2. Configuration des Mises à jour

Les mises à jour peuvent être réalisées depuis un réseau local, directement depuis Internet, ou au travers d'un serveur proxy. Par défaut, BitDefender recherche les mises à jour chaque heure sur Internet et installe celles qui sont disponibles sans vous en avertir.
Pour configurer les paramètres de mise à jour et gérer les serveurs proxy, cliquez sur **Mise à jour > Paramètres** dans la console des paramètres. La fenêtre suivante apparaît :



Configuration des Mises à jour

Les paramètres de mise à jour sont regroupés en quatre catégories **(Paramètres d'emplacement de mise à jour, Paramètres de mise à jour automatique, Paramètres de mise à jour manuelle et Paramètres avancés).** Chaque catégorie est décrite séparément.

12.2.1. Configuration des emplacements de mise à jour

Pour configurer les emplacements de mise à jour, utilisez les options de la catégorie Paramètres d'emplacement de mise à jour.



Note
Ne configurez ces paramètres que si vous êtes connecté à un réseau local qui stocke les signatures de codes malicieux BitDefender localement ou si vous êtes connecté à Internet via un serveur proxy.

Pour effectuer des mises à jour plus fiables et plus rapides, vous pouvez configurer deux **emplacements de mise à jour** : un premier emplacement de mise à jour et un **emplacement alternatif de mise à jour**. Par défaut, ces emplacements sont identiques : http ://upgrade.bitdefender.com.
Pour modifier l'un des emplacements de mise à jour, indiquez l'URL du site miroir local dans le champ URL correspondant à l'emplacement que vous souhaitez modifier.



Note
Nous vous recommandons de configurer le miroir local en tant que premier emplacement de mise à jour et de conserver l'emplacement alternatif de mise à jour inchangé par sécurité, au cas où le miroir local deviendrait indisponible.

Si votre entreprise utilise un serveur proxy pour se connecter à Internet, cochez la case Utiliser un Proxy, puis cliquez sur Gérer les **serveurs proxy** pour configurer les paramètres du proxy.



Note
Pour plus d'informations, reportez-vous à “Gestion des serveurs proxy” (p. 139)

12.2.2. Configuration de la mise à jour automatique

Pour configurer le processus de mise à jour exécuté automatiquement par BitDefender, utilisez les options de la catégorie Paramètres de **mise à jour automatique.**
Vous pouvez spécifier le nombre d'heures entre deux recherches consécutives de mises à jour dans le champ Intervalle de temps. Par défaut, l'intervalle est d'une heure.
Pour déterminer comment le processus de mise à jour automatique doit être exécuté, sélectionnez l'une des options suivantes :
- **Mise à jour silencieuse** - BitDefender télécharge et installe automatiquement la mise à jour de manière transparente pour l'utilisateur.
- **Demander avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, le système demande votre autorisation avant de la télécharger.



Note
L'autorisation vous est demandée avant que la mise à jour ne soit téléchargée, même si vous quittez le Centre de sécurité.

• Demander avant d'installer les mises à jour - chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.



Note
L'autorisation vous est demandée avant que la mise à jour ne soit installée, même si vous quittez le Centre de sécurité.

12.2.3. Configuration de la mise à jour manuelle

Pour déterminer comment la mise à jour manuelle (mise à jour à la demande de l'utilisateur) doit être exécutée, sélectionnez l'une des options suivantes dans la catégorie Paramètres de la mise à jour manuelle :
• Mise à jour silencieuse - la mise à jour manuelle est exécutée automatiquement en tâche de fond, sans l'intervention de l'utilisateur.
• Demander avant de télécharger les mises à jour - chaque fois qu'une mise à jour est disponible, le système demande votre autorisation avant de la télécharger.



Note
L'autorisation vous est demandée avant que la mise à jour ne soit téléchargée, même si vous quittez le Centre de sécurité.

12.2.4. Configuration des paramètres avancés

Pour éviter que les mises à jour de BitDefender n'interfèrent avec votre travail, configurez les options au niveau des Paramètres avancés :
• Patientez pour redémarrer, au lieu de le demander à l'utilisateur - Si une mise à jour nécessite un redémarrage, le produit continuera à utiliser les anciens fichiers jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti qu'il doit redémarrer et ne sera donc pas perturbé dans son travail par la mise à jour de BitDefender.
• Ne pas faire la mise à jour si l'analyse est en cours - BitDefender ne se mettra pas à jour si une analyse est en cours afin de ne pas la perturber.



Note
Si une mise à jour de BitDefender a lieu pendant l'analyse, celle-ci sera interrompue.

• Ne pas mettre à jour si le mode jeu est actif - BitDefender n'effectuera pas de mise à jour si le mode jeu est activé. Ainsi, vous limitez l'influence du produit sur les performances du système lorsque vous jouez.

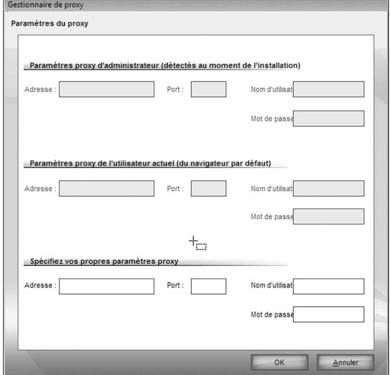
12.2.5. Gestion des serveurs proxy

Si votre entreprise utilise un serveur proxy pour se connecter à Internet, vous devez spécifier les paramètres du Proxy afin que BitDefender puisse se mettre à jour. Sinon, BitDefender utilisera les paramètres du Proxy de l'administrateur qui a installé le produit ou du navigateur par défaut de l'utilisateur actuel, le cas échéant.



Note
Les paramètres du proxy peuvent être configurés uniquement par les utilisateurs possédant des droits d'administrateur ou par des utilisateurs avec pouvoir (des utilisateurs qui connaissent le mot de passe pour accéder aux paramètres du produit).

Pour gérer les paramètres du proxy, cliquez sur Gérer les serveurs proxy. La fenêtre Gestionnaire de Proxy s'affiche.



Gestionnaire de proxy

Il existe trois catégories de paramètres de proxy :

• Paramètres de configuration du proxy (détectés à l'installation) - Paramètres de configuration du Proxy détectés pendant l'installation avec le compte Administrateur ; ces paramètres peuvent être modifiés uniquement si vous êtes connecté avec ce compte. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.

• Paramètres du proxy de l'utilisateur actuel (du navigateur par défaut) - paramètres du Proxy de l'utilisateur actuel provenant du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.



Note
Les navigateurs Web pris en charge sont Internet Explorer, Mozilla Firefox et Opera. Si vous utilisez un autre navigateur par défaut, BitDefender ne pourra pas obtenir les paramètres du proxy de l'utilisateur actuel.

• **Votre propre catégorie de paramètres de proxy** - paramètres de proxy que vous pouvez configurer si vous êtes connecté en tant qu'administrateur.

Voici les paramètres à spécifier :

• **Adresse** - saisissez l'IP du serveur proxy.

• **Port** - saisissez le port utilisé par BitDefender pour se connecter au serveur proxy.

• **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.

• **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

Lors de la tentative de connexion à Internet, chaque catégorie de paramètres de proxy est testée, jusqu'à ce que BitDefender parvienne à se connecter. Tout d'abord, la catégorie contenant vos propres paramètres de proxy est utilisée pour la connexion
Internet. Si elle ne fonctionne pas, ce sont alors les paramètres de proxy détectés lors de l'installation qui sont utilisés. Finalement, s'ils ne fonctionnent pas non plus, les paramètres du proxy de l'utilisateur actuel sont pris sur le navigateur par défaut et utilisés pour la connexion Internet.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre.

Cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

13. CD de secours BitDefender

13.1 Vue d'ensemble

BitDefender internet security 2008 est fourni sur un CD bootable (basé sur LinuxDefender), qui peut être utilisé pour désinfecter un système sans le lancer. Il est recommandé d'utiliser le CD de secours BitDefender à chaque fois que votre système d'exploitation ne fonctionne pas correctement à cause d'une infection virale. Ceci se produit généralement quand vous n'utilisez pas un produit antivirus. La mise à jour de la base de signatures de virus se fait automatiquement, sans intervention de l'utilisateur, à chaque fois que vous lancez le CD de secours BitDefender.
LinuxDefender est une distribution Knoppix remasterisée BitDefender qui intègre les dernières solutions de sécurité BitDefender pour Linux dans le Live CD de GNU/Linux Knoppix, offrant un antivirus de bureau capable d'analyser et de désinfecter les lecteurs de disque dur existants (y compris les partitions Windows NTFS). LinuxDefender peut aussi être utilisée pour restaurer toutes vos données précieuses lorsque Windows ne peut être démarré.

13.2 Configuration requise

Avant de booter sur le CD LinuxDefender, vous devez d'abord vérifier que votre système remplit les conditions suivantes:

Type de processeur :
x86 compatible, minimum 166 MHz pour des performances minimales, un processeur de la génération i686 à 800MHz au moins sera un meilleur choix.

Mémoire :
Mémoire minimum : 512Mo de RAM (1 GB recommandés)

CD-ROM :
LinuxDefender nécessite l'emploi d'un CD ROM et d'un BIOS capable de booter depuis ce CD.

Connexion directe à Internet :
Bien que LinuxDefender puisse être exécuté sans connexion Internet, le processus de mise à jour nécessite un lien HTTP actif pour se télécharger et assurer la meilleure protection possible, même à travers un serveur proxy. La connexion Internet est donc indispensable.CD de secours BitDefender

Résolution graphique :
Carte graphique standard compatible SVGA.

13.3 Fonctionnement de LinuxDefender

Ce chapitre vous explique comment démarrer et arrêter LinuxDefender, analyser votre ordinateur contre les codes malveillants et enregistrer les données de votre PC sur un support amovible si cela s'avère nécessaire. Les applications logicielles qui accompagnent le CD vous offriront la possibilité d'effectuer de nombreuses tâches, mais leur description dépasse toutefois largement le cadre de ce guide d'utilisation.

Lancer LinuxDefender

Pour lancer le CD, configurez les options de votre BIOS pour autoriser le boot sur le CD au démarrage de l'ordinateur, mettez le CD dans le lecteur et redémarrez. Vérifiez bien que votre ordinateur puisse booter sur un CD.
Patientez jusqu'à l'apparition du prochain message et suivez les instructions pour lancer LinuxDefender



Page d'accueil au démarrage

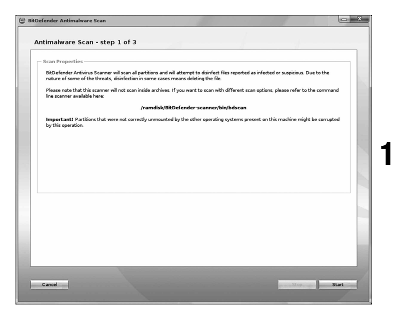
Au démarrage, la mise à jour des signatures de virus est effectuée automatiquement. Cela peut prendre un certain temps.

CD de secours BitDefender
Quand le processus de démarrage sera terminé, vous pourrez utiliser BitDefender Antivirus Scanner.

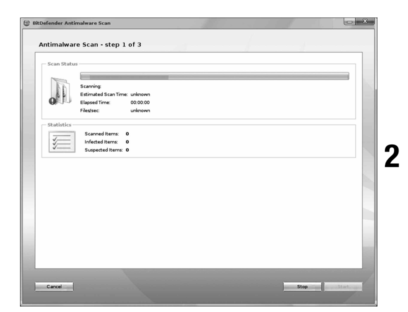


L'interface

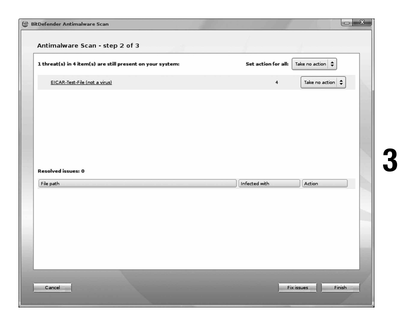
BitDefender Antivirus Scanner analysera toutes les partitions et essaiera de désinfecter les fichiers reportés comme infectés ou suspects. En raison de la nature de certaines menaces, la désinfection reviendra dans certains cas à supprimer le fichier.



1



2



3



4

Le scanner n'analysera pas à l'intérieur des archives.

Si vous souhaitez lancer une analyse particulière, contrôler des archives, etc., il est possible de passer en ligne de commande. Les options de paramétrages sont dès lors accessibles par la commande suivante :

/ramdisk/BitDefender_Scanner/bin/bdscan

Arrêter LinuxDefender

Vous pouvez éteindre votre ordinateur en toute sécurité en sélectionnant Quitter dans le menu contextuel LinuxDefender (double-cliquez pour l'ouvrir) ou en lançant la commande d'arrêt halt depuis un terminal.



Choisissez "**Sortir**" de LinuxDefender
BitDefender internet security 2008
Lorsque LinuxDefender a terminé de fermer tous les programmes, il affiche un écran similaire à l'illustration suivante. Vous pouvez retirer le CD pour démarrer depuis votre disque dur. Vous pouvez maintenant éteindre votre ordinateur ou le redémarrer.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspe
) (aio/0) Done.
Waiting for processes to finish.......................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.......................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes]._
```

Patientez jusqu'à l'apparition de ce message quand vous fermez le programme.

14. Support Technique Editions Profil / BitDefender :

Editions Profil et BitDefender s'efforcent de toujours vous fournir des réponses rapides et précises à vos questions.
Le centre de support en ligne, dont vous trouverez les coordonnées ci-dessous, est actualisé en continu et vous donne accès aux réponses aux questions les plus fréquemment posées.

Vous disposez de plusieurs moyens pour obtenir de l'aide concernant votre produit :

1. Mise à disposition d'une foire aux questions sur le site BitDefender :
http://www.bitdefender.fr/site/KnowledgeBase/faq/

2. Support technique par email :
Si votre problème n'est toujours pas résolu après avoir utilisé l'aide en ligne, vous pouvez alors nous envoyer une demande personnalisée. Merci d'utiliser pour cela le formulaire présent sur notre site dans le volet "Assistance Technique" à droite de la page de "foire aux questions" de votre produit.

3. Par téléphone, du lundi au vendredi :

Pour la France : 08.92.950.950 (0,34   TTC / min)

Pour la Belgique : 02 290.83.04

Pour la Suisse : 0900 000 118

4. Par prise de contrôle à distance
Cette possibilité requiert de contacter le support téléphonique. Suivant le problème, nos techniciens vous proposeront de prendre à distance le contrôle de votre ordinateur afin de solutionner votre problème et vous éviter ainsi de devoir réaliser vous-même les manipulations.

5. Par chat online – Accessible 7j/7 – 365j/an
Ce service permet de vous mettre en relation direct avec un technicien y compris durant les jours fériés ou la nuit. Pour y accéder, veuillez saisir l'adresse ci-dessous dans votre navigateur :
http://www.bitdefender.com/site/KnowledgeBase/liveAssistance
Attention, ce service est un service international, assuré majoritairement en anglais.


ÉDITIONS
PROFIL
www.editions-profil.eu


www.bitdefender.fr